Plan de Reprise d’Activité (PRA)

Sommaire

I - Détaillez, pour chacun des points

1. Évaluation de l'incident

Au début il faut surtout comprendre ce qui s'est passé. Les clients peuvent appeler ou envoyer un message car leur site ne marche plus. Ils peuvent aussi avoir un message d'erreur. La DSI doit récupérer ces informations et prévenir la direction.

De leur côté les administrateurs systèmes et réseaux regardent l'état du serveur. Ils vérifient les logs les services qui sont tombés les accès et les sauvegardes. Les développeurs peuvent vérifier les sites web les bases de données et les applications. Le but est de savoir si l'attaque touche seulement le serveur ou aussi les données.

Les personnes concernées sont les clients la DSI la direction l'équipe système et réseau les développeurs et si besoin l'hébergeur ou un prestataire en sécurité.

2. Communication interne et externe

Il faut communiquer rapidement mais sans raconter des choses pas encore vérifiées. En interne la DSI prévient la direction les techniciens et le service client. Comme ça tout le monde part avec la même information.

Pour les clients il faut envoyer un premier message pour expliquer qu'il y a un incident de sécurité. Il faut aussi dire que certains services peuvent être indisponibles. Je pense qu'il ne faut pas donner trop de détails techniques sur l'attaque car ça peut poser un risque.

Si des données personnelles ou bancaires ont été touchées l'entreprise doit aussi vérifier ses obligations légales. Par exemple elle peut devoir prévenir la CNIL.

3. Activation du PRA et équipe de crise

Quand l'incident est confirmé la direction et la DSI activent le PRA. Il faut créer une équipe de crise pour que les actions soient organisées.

La DSI coordonne le travail. Les administrateurs systèmes et réseaux s'occupent du serveur de secours et de l'infrastructure. Les développeurs s'occupent des sites et des tests. Le service client répond aux clients. La direction garde la validation des décisions importantes surtout pour la communication.

4. Priorisation des services critiques

On ne peut pas tout remettre en ligne en même temps. Il faut donc choisir ce qui est le plus important.

Il faut commencer par les sites qui contiennent des paiements ou des données sensibles. Ensuite on remet les sites les plus importants pour les clients. Après on remet les services internes utiles pour travailler. Les sites moins urgents peuvent attendre un peu.

Cette décision doit être faite avec la DSI la direction le service client et les équipes techniques car ils n'ont pas tous la même vision du problème.

5. Mise en place d'un mode dégradé

Pendant la préparation du serveur de secours il faut quand même informer les utilisateurs. On peut mettre une page de maintenance ou une redirection DNS vers une page temporaire.

Le but est d'éviter que les clients pensent que leur site a disparu ou que personne ne s'en occupe. Si une solution de contournement existe le service client peut aussi la donner aux clients même si ce n'est que temporaire.

Les administrateurs gèrent la redirection ou la page temporaire. Les développeurs peuvent aider pour l'affichage.

6. Mise en place du nouvel environnement de production

Comme le serveur principal est compromis il ne faut pas repartir dessus directement. Il faut installer un environnement propre sur le serveur de secours.

Les administrateurs installent le système les mises à jour les services web la base de données les certificats SSL et les règles de pare-feu. Ils doivent aussi vérifier les comptes et les droits pour ne pas remettre une faille.

La DSI suit l'avancement et vérifie que le nouvel environnement peut remplacer la production sans prendre trop de risques.

7. Restauration des données

Une fois le serveur de secours prêt les données sont restaurées depuis les sauvegardes hors site. C'est important que les sauvegardes soient à jour et non compromises. Sinon le PRA ne servirait pas à grand chose.

Avant de restaurer les administrateur doivent vérifier que les sauvegardes sont correctes. Ensuite ils remettent les fichiers et les bases de données. Les développeurs vérifient après que les sites fonctionnent bien avec les données restaurées.

8. Rétablissement des services

Les services doivent être remis en ligne petit à petit. Il vaut mieux commencer par les plus critiques au lieu de tout ouvrir en même temps.

Les administrateurs redémarrent les services web les bases de données le DNS et la supervision. Les développeurs vérifient les configurations des sites. La DSI donne l'accord pour remettre les services en production.

9. Vérification et tests

Avant de dire que tout est revenu il faut tester. Les administrateurs testent le réseau les certificats les log la supervision et les performances.

Les développeurs testent les pages importantes les formulaires les connexions les paiements et l'accès aux bases de données. Si possible on peut demander à quelques clients de tester leur site car leur retour peut montrer des problèmes qu'on n'a pas vu.

10. Communication pendant la reprise

Quand une partie des services remarche il faut refaire un message aux clients. Il faut expliquer que la reprise est en cours. Il faut aussi dire que certains services sont déjà disponibles et que les contrôles continuent.

La DSI donne l'état technique. La direction valide le message et le service client l'envoie.

11. Retour à la normale

Le retour à la normale peut être annoncé quand les services principaux fonctionnent et que les tests sont bons.

Il faut quand même surveiller pendant quelques jours car un problème peut apparaître après la remise en ligne. Les administrateurs regardent les logs et les alertes. Les développeurs corrigent les derniers bugs si besoin.

12. Communication externe finale

Quand tout est stabilisé OmniWeb doit envoyer un dernier mail aux clients. Le mail confirme le retour à la normale. Il explique rapidement ce qui a été fait et présente des excuses pour la gêne.

Il faut aussi dire qu'une surveillance reste en place et qu'un retour d'expérience sera fait après l'incident.

13. Revue post-incident

Après l'incident il faut faire une réunion pour voir ce qui a bien marché et ce qui a posé problème. Ça permet d'améliorer l'organisation pour la prochaine fois.

La DSI organise la réunion. Les administrateurs expliquent la partie serveur et réseau. Les développeurs parlent des problèmes sur les applications. Le service client remonte les retours des clients. Après ça la direction décide des améliorations à faire.

14. Mise à jour du PRA

Le PRA doit être mis à jour avec ce qui a été appris pendant l'incident. On peut ajouter les contacts utiles ,les délais réels ,les commandes importantes et les étapes qui manquaient.

La DSI modifie le document. Les équipes techniques ajoutent des info précises. La direction valide la nouvelle version.

15. Formation et sensibilisation

Pour finir il faut sensibiliser les équipes. Ce n'est pas seulement un problème technique car une attaque peut aussi venir d'une erreur humaine.

On peut faire une sensibilisation sur le phishing ,les mots de passe, les droits d'accès et les sauvegardes et la façon de signaler un problème. Tout le personnel est concerné et pas seulement les informaticiens.

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

Pour l'évaluation de l'incident je mettrais environ 1 h à 2 h. Pendant ce temps plusieurs personnes peuvent travailler en même temps. Les administrateurs regardent les logs. Les développeurs regardent les sites. La DSI regroupe les informations.

La première communication peut prendre environ 30 min à 1 h. Elle peut être préparée pendant l'analyse mais il faut que la direction valide avant l'envoi .

L'activation du PRA prend environ 30 min. C'est surtout une décision de la DSI

La priorisation des services peut prendre environ 1 h .

Le mode dégradé peut prendre 1 h à 2 h. Cette partie peut aussi être faite en parallèle pendant que le serveur de secours est installé.

La mise en place du nouvel environnement peut prendre entre 3 h et 6 h.

La restauration des données peut prendre 2 h à 5 h.

Le rétablissement des services peut prendre 1 h à 3 h. Il faut le faire progressivement pour éviter de remettre un service qui ne fonctionne pas.

Les tests peuvent prendre 1 h à 3 h. Les tests réseau système et applicatifs peuvent être faits en parallèle.

La communication après reprise partielle prend environ 30 min. La communication finale prend aussi environ 30 min .

Le retour à la normale peut prendre 2 h à 4 h car il faut vérifier que les services restent stables.

La revue post-incident peut durer environ 2 h. La mise à jour du PRA peut prendre 2 h à 4 h. La sensibilisation peut prendre 1 h à 2 h .

Au total pour remettre les services principaux on peut estimer entre 10 h et 24 h. Les tâches qui peuvent se faire en parallèle sont surtout l'analyse et la communication, la préparation du serveur avec mode dégradé et les tests.

III - Rédigez intégralement les mails à destination de l’ensemble de la clientèle sur les étapes de communication.

Mail 1 : début de l'incident

Objet : Information sur l'indisponibilité de nos services

Bonjour,

Nous vous informons qu'un incident de sécurité touche actuellement une partie de notre infrastructure. Certains services hébergés par OmniWeb peuvent donc être temporairement indisponibles.

Nos équipes techniques sont mobilisées pour analyser la situation et préparer la reprise. Pour le moment nous préférons sécuriser correctement l'environnement avant de remettre les services en ligne.

Nous vous tiendrons informés dès que nous aurons plus d'informations confirmées. Si vous constatez un problème particulier sur votre site vous pouvez contacter notre support.

Nous sommes désolés pour la gêne occasionnée et merci pour votre compréhension.

Cordialement,

L'équipe OmniWeb

Mail 2 : pendant la reprise

Objet : Point d'avancement sur la reprise des services

Bonjour,

Nous revenons vers vous concernant l'incident signalé précédemment. Notre Plan de Reprise d'Activité a été activé et nos équipes travaillent actuellement sur un serveur de secours.

Les sauvegardes utilisées sont récentes stockées hors site et n'ont pas été compromises. La restauration est faite progressivement en commençant par les services les plus importants.

Certains services peuvent revenir en ligne avant d'autres. Des tests sont réalisés avant chaque remise en service pour vérifier le bon fonctionnement.

Nous continuerons à vous informer jusqu'au retour complet à la normale.

Cordialement,

L'équipe OmniWeb

Mail 3 : reprise partielle

Objet : Rétablissement progressif des services OmniWeb

Bonjour,

Nous vous informons que plusieurs services OmniWeb sont de nouveau disponibles. La reprise continue progressivement sur un environnement reconstruit et contrôlé par nos équipes.

Des vérifications sont encore en cours. Il est donc possible que certaines fonctionnalités soient encore indisponibles ou que de petites interruptions aient lieu pendant les derniers contrôles.

Si vous remarquez une anomalie sur votre site merci de la signaler au support avec l'adresse du site l'heure du problème et une courte description.

Merci pour votre patience.

Cordialement,

L'équipe OmniWeb

Mail 4 : retour à la normale

Objet : Retour à la normale des services OmniWeb

Bonjour,

Nous vous confirmons que les services OmniWeb sont revenus à un fonctionnement normal après l'incident de sécurité.

La reprise a été faite à partir de sauvegardes récentes et non compromises. Nos équipes ont reconstruit l'environnement restauré les données et réalisé les tests nécessaires avant la remise en service.

Une surveillance renforcée reste en place pour détecter rapidement toute anomalie. Un retour d'expérience sera aussi fait en interne pour améliorer nos procédures.

Nous vous présentons nos excuses pour la gêne occasionnée et nous vous remercions pour votre compréhension.

Cordialement,

L'équipe OmniWeb