



Plan de continuité des activités

Semana SAS Mise à

jour précédente : 05/07/2022

Révision : Albert Reynaud et Nicolas Cosmes

Point de contact : Albert Reynaud - albert@semana.io

Aspects de la sécurité de l'information dans la gestion de la continuité des activités

Continuité de la sécurité de l'information

Semana héberge l'infrastructure de ses produits chez des fournisseurs d'infrastructure de premier plan, actuellement Google Cloud Platform, qui fournissent des niveaux élevés de disponibilité physique et de réseau et maintiennent divers niveaux de sécurité vérifiés, y compris SOC 2 Type II et la conformité ISO 27001.

Licenciements

Nos principaux fournisseurs nous garantissent un temps de disponibilité des installations compris entre 99,95 % et 100,00 % et les deux fournisseurs assurent une redondance minimale de N+1 pour tous les services d'alimentation électrique, de réseau et de chauffage, de ventilation et de climatisation.

Les données sont répliquées et sauvegardées dans plusieurs entrepôts de données durables répartis dans des centres de données afin d'ajouter un niveau supplémentaire de protection hors site géographiquement dispersé. Les applications dorsales sont exploitées dans 3 zones de disponibilité de notre fournisseur d'hébergement.

Vérifier, examiner et évaluer la continuité de la sécurité de l'information

Les tests de continuité des activités font partie du processus normal de Semana. Nos processus de récupération sont validés en permanence dans le cadre des processus normaux de maintenance et d'assistance. Nous utilisons des services gérés qui nous permettent de mettre rapidement en place des environnements. Nous utilisons exactement les mêmes procédures dans un scénario de reprise, ce qui nous permet de pratiquer notre processus de reprise tous les jours.

Plan de réponse aux incidents

Introduction

Semana met en œuvre un processus de réponse aux incidents de sécurité de l'information afin de détecter, de répondre et de signaler systématiquement les incidents, de minimiser les pertes et les destructions, d'atténuer les faiblesses qui ont été exploitées et de rétablir la fonctionnalité du système d'information et la continuité des activités dans les meilleurs délais.

Le processus de réponse aux incidents porte sur les points suivants

- Surveillance continue des menaces au moyen de systèmes de détection d'intrusion (IDS) et d'autres applications de surveillance ;
- Mise en place d'une équipe d'intervention en cas d'incident lié à la sécurité de l'information ;
- Mise en place de procédures claires pour l'identification, la réponse, l'évaluation, l'analyse et le suivi des incidents liés à la sécurité de l'information ;
- la formation, l'éducation et la sensibilisation du personnel aux incidents liés à la sécurité de l'information et aux réponses à y apporter ; et
- Faciliter une communication claire des incidents de sécurité de l'information avec les parties prenantes internes et externes.

Classification des événements liés à la sécurité

La réponse aux incidents de Semana classe les événements liés à la sécurité dans les catégories suivantes :

- **Événements** Tout événement observable lié à la sécurité informatique dans un système ou un réseau et ayant des conséquences négatives. Exemples :
 - Défaillance d'un composant matériel entraînant des interruptions de service.
 - Erreur logicielle provoquant des interruptions de service.
 - Instabilité générale du réseau ou du système.
- **Précurseurs** Signe qu'un incident peut se produire à l'avenir. Exemples :
 - Système de surveillance présentant un comportement inhabituel.
 - Les alertes du journal d'audit ont indiqué que plusieurs tentatives de connexion avaient échoué.
 - Des courriels suspects ciblant des membres spécifiques du personnel de Semana ayant un accès administratif aux systèmes de production.
- **Indices** Signes indiquant qu'un incident a pu se produire ou est en train de se produire. Exemples :
 - L'IDS alerte en cas de fichiers système modifiés ou d'accès inhabituels au système.
 - Alertes antivirus pour les fichiers infectés.
 - Trafic réseau excessif dirigé vers des lieux géographiques inattendus.
- **Incidents** Violation des politiques de sécurité informatique ou des politiques d'utilisation acceptable, entraînant souvent des violations de données. Exemples :
 - Divulcation non autorisée d'ePHI.

- Modification ou destruction non autorisée des données à caractère personnel.
- Une violation de données commise par une entité interne ou externe.
- Une attaque par déni de service (DoS) qui rend un service critique inaccessible.

Les employés de Semana doivent signaler toute activité non autorisée ou suspecte observée sur les systèmes de production ou associée aux systèmes de communication connexes (tels que le courrier électronique ou Slack). En pratique, cela signifie qu'il faut garder un œil sur les événements de sécurité et informer l'équipe de sécurité de Semana de tout précurseur ou indice observé dès qu'il est découvert.

Procédure de gestion des incidents

Tous les événements, précurseurs, indications et incidents ("problèmes"), connus ou suspectés, doivent être traités conformément à la procédure de gestion des incidents ("PGI"). La PGI se compose de (jusqu'à) cinq phases. Ces phases sont les suivantes : L'identification, le confinement, l'éradication, le rétablissement et le suivi. En fonction du type de problème présenté, certaines phases de la PGI peuvent être omises. Dans le cas contraire, les phases doivent être exécutées dans l'ordre indiqué ci-dessous.

- **Phase d'identification** : Dans cette phase, l'équipe de sécurité de Semana est informée d'un problème de sécurité potentiel et détermine si une enquête plus approfondie et une réponse sont nécessaires.
 - Dès qu'ils sont observés, les membres de Semana signalent les problèmes de sécurité potentiels. Les rapports peuvent être faits directement à la direction, à l'équipe de sécurité de Semana, ou au Directeur Technique. Les rapports peuvent également être faits par email, par téléphone ou par chat sécurisé.
 - La personne qui reçoit le rapport doit en informer un membre de l'équipe de sécurité de Semana (si ce n'est déjà fait).
 - L'équipe de sécurité de Semana est chargée de classer le problème signalé comme un événement, un précurseur, une indication ou un incident.
 - S'il s'agit d'un événement, d'un précurseur ou d'une indication, l'équipe de sécurité de Semana transmettra le problème à la ressource informatique appropriée pour qu'elle le résolve. Cette ressource peut également être un contractant ou une ressource technique externalisée, si nécessaire.
 - S'il s'agit d'un incident, l'équipe de sécurité de Semana en informera la direction.
 - Pour les incidents de sécurité non techniques, l'équipe de sécurité de Semana mènera une enquête, mettra en place des mesures préventives et résoudra l'incident. Une fois l'enquête terminée, l'équipe de sécurité de Semana saute les phases de confinement, d'éradication et de récupération et passe à la phase de suivi.
 - Pour les incidents de sécurité technique, l'équipe de sécurité de Semana passera à la phase de confinement.
- **Phase de confinement** : Au cours de cette phase, l'équipe de sécurité de Semana tente de contenir le problème de sécurité confirmé. Il est de la plus haute importance que des notes détaillées soient prises pendant la phase de confinement.

l'ensemble de ce processus.

- L'équipe de sécurité de Semana examine toutes les informations recueillies jusqu'à présent par les personnes qui ont enquêté sur le problème.
 - L'équipe de sécurité de Semana prendra les mesures suivantes :
 - Se connecter de manière sécurisée au système concerné par le biais d'une connexion de confiance.
 - Récupérer toutes les données volatiles du système affecté.
 - Déterminer l'intégrité relative et l'opportunité de sauvegarder le système.
 - Le cas échéant, sauvegarder le système.
 - Le cas échéant, changer le(s) mot(s) de passe du (des) système(s) concerné(s).
 - Déterminer s'il est possible de poursuivre en toute sécurité les opérations avec le(s) système(s) affecté(s).
 - S'il est sûr, l'équipe de sécurité de Semana autorisera le système à continuer de fonctionner et passera à la phase de suivi.
 - L'équipe de sécurité de Semana informera en permanence la direction générale des progrès réalisés.
 - L'équipe de sécurité de Semana continuera à notifier les clients concernés avec des mises à jour pertinentes si nécessaire.
-
- **Phase d'éradication** : Pendant la phase d'éradication, l'équipe de sécurité de Semana éliminera la cause du problème de sécurité et les risques de sécurité qui en résultent, qui se trouvent maintenant sur le(s) système(s) affecté(s). L'équipe de sécurité de Semana prendra les mesures suivantes :
 - Déterminer les symptômes et la cause liés au(x) système(s) affecté(s).
 - Renforcer les défenses entourant le(s) système(s) affecté(s), si possible (une évaluation des risques peut être nécessaire et peut être déterminée par l'équipe de sécurité de Semana).
 - Remédiation ("correction") de tout problème de sécurité dans le système affecté, par exemple en supprimant les services inutilisés ou en appliquant des techniques générales de durcissement de l'hôte.
 - Procéder à une évaluation détaillée des vulnérabilités afin de vérifier que toutes les failles ou lacunes susceptibles d'être exploitées ont été comblées. Si d'autres problèmes ou symptômes sont identifiés, prendre les mesures préventives appropriées afin d'éliminer ou de minimiser les risques de compromission à l'avenir.
 - Mettre à jour la documentation avec les informations tirées de l'évaluation de la vulnérabilité, y compris la cause, les symptômes et la méthode utilisée pour résoudre le problème avec le(s) système(s) affecté(s).
 - Informer l'encadrement supérieur des progrès réalisés.
 - Continuer à informer les clients concernés en leur communiquant les mises à jour nécessaires.
 - Passer à la phase de récupération.
-
- **Phase de rétablissement** : La phase de rétablissement couvre la remise en service du ou des systèmes affectés après que les éventuelles failles de sécurité ont été corrigées.
 - L'équipe de sécurité de Semana détermine si le(s) système(s) affecté(s) a (ont) été modifié(s) de quelque manière que ce soit. Si ce n'est pas le cas,

elle passe à la phase de suivi.

- Si le(s) système(s) concerné(s) a (ont) été modifié(s) :
 - L'équipe de sécurité de Semana rétablit le système dans son fonctionnement normal (c'est-à-dire le dernier état ou la dernière configuration "bonne" connue).

- Une fois le système restauré, l'équipe de sécurité de Semana vérifie qu'il fonctionne comme prévu ou qu'il a fonctionné dans le passé.
 - Si le fonctionnement du ou des systèmes a été interrompu (c'est-à-dire que le ou les systèmes ont été mis hors ligne ou retirés du réseau pendant le triage), redémarrer le ou les systèmes restaurés et validés et surveiller leur comportement.
 - Si le système n'a subi aucune modification, mais qu'il a été mis hors ligne (c'est-à-dire que les opérations ont été interrompues), redémarrez le système et vérifiez qu'il se comporte correctement.
 - Mettre à jour la documentation avec les détails qui ont été déterminés au cours de cette phase.
 - Informer l'encadrement supérieur des progrès réalisés.
 - Continuer à informer les clients concernés si nécessaire.
 - Passer à la phase de suivi.
- **Phase de suivi :** La phase de suivi représente la fin de la procédure de gestion des incidents et consiste à examiner le problème de sécurité pour en tirer des "enseignements" et déterminer si la procédure suivie aurait pu être améliorée de quelque manière que ce soit. Tous les problèmes de sécurité sont examinés peu de temps après leur résolution afin de déterminer si la réponse peut être améliorée.
 - Les personnes chargées de répondre au problème de sécurité (c'est-à-dire l'équipe de sécurité de Semana et toutes les ressources techniques pertinentes en matière de sécurité) se réunissent pour examiner la documentation recueillie pour le problème de sécurité.
 - L'équipe de sécurité de Semana documente les "leçons apprises" (soit dans un document indépendant, soit dans le présent plan de réponse aux incidents, soit dans un manuel de réponse aux incidents). Dans le cadre de ce processus de documentation, le coût et l'impact du problème de sécurité pour Semana et les améliorations apportées à la sécurité doivent être discutés.
 - L'équipe de sécurité de Semana communique ses conclusions à la direction générale pour approbation et pour la mise en œuvre de toute recommandation formulée après l'examen de la question de la sécurité.
 - L'équipe de sécurité de Semana met en œuvre toutes les recommandations approuvées par la direction générale.
 - Après avoir mis en œuvre les recommandations approuvées, l'équipe de sécurité de Semana clôt la question de sécurité.

Équipe de sécurité Semana

En plus des autres responsabilités liées à la sécurité, l'équipe de sécurité de Semana est responsable de l'exécution de la procédure de gestion des incidents. En particulier, au moins un des employés suivants de Semana doit être impliqué dans l'exécution de la procédure de gestion des incidents :

- Directeur technique
- 2 développeurs seniors

Plan de reprise après sinistre

Introduction

Le présent plan de reprise après sinistre ("PRS") établit les procédures de reprise de Semana à la suite d'une perturbation résultant d'un sinistre. Les types de désastres envisagés par ce plan incluent les désastres naturels, les troubles politiques, les désastres d'origine humaine, les menaces humaines externes et les activités malveillantes internes. Ce plan est maintenu par l'équipe de sécurité de Semana et par le directeur de la technologie de Semana.

Objectifs

Les objectifs de ce plan sont les suivants :

1. Maximiser l'efficacité des opérations d'urgence grâce à un plan établi qui comprend les phases de notification, de rétablissement et de reconstitution.
2. Identifier les activités, les ressources et les procédures nécessaires pour répondre aux besoins de traitement de Semana en cas d'interruption prolongée des opérations normales.
3. Identifier et définir l'impact des interruptions sur les systèmes de Semana.
4. Attribuer des responsabilités au personnel désigné et fournir des orientations pour le rétablissement de Semana pendant les périodes prolongées d'interruption des opérations normales.
5. Assurer la coordination avec les autres membres du personnel de Semana qui participeront aux stratégies de planification d'urgence.
6. Assurer la coordination avec les points de contact externes et les fournisseurs qui participeront aux stratégies de planification d'urgence.

L'objectif de point de récupération (RPO) de ce plan est de 24 heures. L'objectif de temps de récupération (RTO) de ce plan est de 48 heures.

Types de systèmes

Du point de vue de la reprise après sinistre, Semana définit deux catégories de systèmes :

1. **Systèmes critiques** : Ces systèmes hébergent des serveurs d'applications et des serveurs de bases de données ou sont nécessaires au fonctionnement des systèmes qui hébergent des serveurs d'applications et des serveurs de bases de données. Ces systèmes, s'ils sont indisponibles, affectent l'intégrité des données et doivent être restaurés, ou faire l'objet d'un processus de

restauration, immédiatement après leur mise en service.

deviennent indisponibles. Les bases de données et les index de Semana sont des exemples de systèmes critiques.

2. **Systèmes non critiques.** Il s'agit de tous les systèmes qui ne sont pas considérés comme critiques selon la définition ci-dessus. Ces systèmes, bien qu'ils puissent affecter les performances et la sécurité globale des systèmes critiques, n'empêchent pas les systèmes critiques de fonctionner et d'être accessibles de manière appropriée. Les systèmes non critiques sont restaurés avec une priorité moindre que les systèmes critiques. Les serveurs d'analyse sont des exemples de systèmes non critiques.

Ligne de succession

L'ordre de succession suivant garantit que le pouvoir de décision pour le PRD est ininterrompu. Le CTO est chargé d'assurer la sécurité du personnel et l'exécution des procédures documentées dans le présent DRP. Si le CTO n'est pas en mesure d'assumer l'autorité générale ou s'il choisit de déléguer cette responsabilité à un successeur, c'est le directeur général qui assumera cette fonction. La liste de contacts ci-dessous permet d'établir des contacts en cas de mise en œuvre du plan d'urgence.

Nicolas Cosmes CTO, nicolas@semana.co & Albert Reynaud, CEO, albert@semana.io

Procédure de reprise après sinistre

- **Phase de notification :** Cette phase concerne les mesures initiales prises pour détecter et évaluer les dommages causés par une perturbation de Semana. La séquence de notification est décrite ci-dessous :
 - Le premier intervenant doit avertir le CTO.
 - Le CTO doit informer les membres de l'équipe et leur demander d'évaluer l'étendue des dégâts et le temps de rétablissement estimé.
 - Sur la base de l'évaluation des dommages, si Semana est indisponible pour les clients pendant plus de 24 heures, le CTO déclarera qu'une catastrophe s'est produite et que la procédure de reprise après sinistre a été activée. Le CTO a également le pouvoir discrétionnaire d'activer la procédure de reprise après sinistre sur la base d'autres critères.
 - Une fois la procédure de reprise après sinistre activée, le CTO doit informer l'ensemble du personnel et la direction générale de l'état général de l'incident. La notification peut se faire par message, par courriel ou par téléphone. Le CTO peut également informer l'équipe opérationnelle de Semana si le sinistre concerne les locaux de Semana ou les employés de Semana.
 - Si la procédure de reprise après sinistre n'a pas été activée, les phases de reprise et de reconstitution ne seront pas exécutées. Au lieu de cela, le CTO et les membres de l'équipe nécessaires effectueront toutes les tâches appropriées dans le cadre du plan d'intervention en cas d'incident de Semana.

- **Phase de récupération :** Cette phase couvre la récupération de l'application sur un site alternatif. Si le sinistre concerne à la fois des systèmes critiques et des systèmes non critiques, l'équipe de sécurité de Semana peut donner la priorité à la récupération des systèmes critiques et passer à la phase de reconstitution pour les systèmes critiques avant que les systèmes non critiques n'aient terminé la phase de récupération. Cette phase comprend les tâches suivantes, dont certaines peuvent être exécutées en parallèle :
 - Contacter les partenaires et les clients concernés
 - Évaluer les dommages causés aux environnements touchés
 - Commencer la réplication du nouvel environnement à l'aide de scripts automatisés et testés Tester le nouvel environnement à l'aide de tests pré-écrits
 - Tester les fonctionnalités de journalisation, de sécurité et d'alerte
 - Vérifier que les systèmes sont correctement corrigés et mis à jour.
 - Déployer le nouvel environnement dans la production
 - Mise à jour du DNS dans le nouvel environnement
 - Si le sinistre concerne les locaux de Semana ou les employés de Semana, l'équipe d'exploitation de Semana exécutera toutes les tâches nécessaires à la récupération de l'application sur un autre site.

- **Phase de reconstitution :** Cette phase comprend les activités nécessaires pour rétablir les opérations de Semana sur le site d'origine (ou pour déplacer définitivement les opérations sur le nouveau site, si nécessaire). Si la catastrophe concerne à la fois des systèmes critiques et des systèmes non critiques, l'équipe de sécurité de Semana peut donner la priorité à la reconstitution des systèmes critiques avant de commencer la reconstitution des systèmes non critiques. Cette phase comprend les tâches suivantes, dont certaines peuvent être exécutées en parallèle :
 - Commencer la réplication du nouvel environnement à l'aide de scripts automatisés et testés.
 - Tester le nouvel environnement à l'aide de tests pré-écrits
 - Tester les fonctionnalités de journalisation, de sécurité et d'alerte
 - Vérifier que les systèmes sont correctement corrigés et mis à jour.
 - Déployer le nouvel environnement dans la production
 - Mise à jour du DNS dans le nouvel environnement
 - Si la catastrophe concerne les locaux de Semana ou les employés de Semana, l'équipe opérationnelle de Semana exécutera toutes les tâches nécessaires pour rétablir les activités de Semana sur le site d'origine (ou pour transférer définitivement les activités sur le nouveau site, si nécessaire).