Plan de Réponse aux Incidents cyber

1. Introduction

Ce plan de réponse aux incidents vise à fournir des directives pour la gestion et la réponse aux incidents de sécurité affectant Buildingerie. L'objectif est de minimiser l'impact des incidents de sécurité sur les utilisateurs, les données et les opérations de l'application.

2. Objectifs

- **Détection rapide** : Identifier les incidents de sécurité dès qu'ils se produisent.
- **Réponse efficace** : Réagir de manière appropriée pour contenir et atténuer les effets de l'incident.
- **Récupération proactive** : Effectuer des changements majeurs dès la remédiation. Nous choisissons d'investir durablement pour réapproprier le pilotage et la défense de votre système d'information.
- **Prévention future** : Apprendre des incidents pour améliorer la sécurité et prévenir des incidents similaires.

3. Équipe de Réponse aux Incidents (ERI)

L'ERI est composée de membres clés de l'organisation, chacun ayant des rôles et des responsabilités spécifiques :

- **Coordinateur de la réponse aux incidents** : Supervise l'ensemble du processus de réponse.
- **Analystes de sécurité** : Enquêtent sur l'incident et fournissent des analyses techniques, conseille sur les implications légales et la conformité.
- **Développeurs** : Corrigent les vulnérabilités dans le code.
- **Administrateurs système** : Gèrent l'infrastructure et appliquent les correctifs nécessaires.
- **Communication** : Gère la communication interne et externe concernant l'incident.
- **Juridique** : Conseille sur les implications légales et la conformité.

4. Identification des Incidents

- **Sources de détection** : Journaux de logs, rapports des utilisateurs, alertes de sécurité.
- **Critères d'identification** : Activité suspecte, accès non autorisé, anomalies dans le comportement de l'application.

5. Classification des Incidents

Les incidents sont classés en fonction de leur gravité et de leur impact :

- **Critique** : Compromet les données sensibles des utilisateurs ou l'intégrité de l'application.
- **Élevée** : Affecte une partie importante des utilisateurs ou des fonctionnalités.
- **Moyenne** : Impact limité sur les utilisateurs et les fonctionnalités.
- **Faible** : Impact minimal et facilement réversible.

6. Confinement

- **Confinement à court terme** : Isolation de l'incident pour empêcher une propagation ultérieure (exemples : déconnexion des systèmes compromis, blocage des adresses IP malveillantes).
- **Confinement à long terme** : Mise en place de correctifs temporaires et surveillance accrue pour prévenir de nouvelles occurrences pendant l'enquête.

7. Éradication

- **Analyse des causes** : Identification de la cause de l'incident.
- **Suppression des menaces** : Élimination des logiciels malveillants, correction des vulnérabilités.
- **Restitution des systèmes** : Remise en état des systèmes compromis avec des versions sécurisées.

8. Récupération

- **Restauration des services** : Remise en ligne des services après vérification de leur sécurité.
- **Tests de validation** : Vérification que les systèmes restaurés sont exempts de vulnérabilités et fonctionnent normalement.
- **Surveillance accrue** : Surveillance renforcée des systèmes pour détecter toute activité suspecte post-récupération.

9. Communication

- **Interne** : Informations régulières aux équipes internes sur la progression de la réponse à l'incident.
- **Externe** : Notifications aux utilisateurs affectés, rapports aux autorités si nécessaire, communication avec les médias si pertinent.

10. Documentation, Apprentissage, Partage

- **Rapport d'incident** : Documentation détaillée de l'incident, des actions entreprises, et des leçons apprises.
- **Révision post-incident** : Analyse post-mortem pour identifier les améliorations à apporter aux procédures de sécurité.
- **Formation et sensibilisation** : Mises à jour des formations de sécurité basées sur les leçons apprises.
- **Partage de connaissances** : Mettre à disposition des entreprises votre plan d’actions avec les bonnes et mauvaises décisions prises. Pour enrichir la compréhension des incidents cyber d’autres entreprises.

11. Mise à Jour du Plan

- **Revue régulière** : Mise à jour périodique du plan pour refléter les nouvelles menaces et les changements dans l'infrastructure ou les opérations.
- **Simulations d'incidents** : Exercices réguliers pour tester et améliorer l'efficacité du plan de réponse aux incidents.

Conclusion

Un plan de réponse aux incidents bien structuré et régulièrement mis à jour est crucial pour la sécurité et la résilience de l'application Buildingerie. En suivant ces étapes, l'organisation peut minimiser les impacts des incidents de sécurité et renforcer la confiance des utilisateurs dans la plateforme.

Document externe utile

CYBERATTAQUES ET REMÉDIATION LES CLÉS DE DÉCISION (ANSSI)