aDvens

Security for the greater good

Défacement de site internet

Méthodologie de réponse à incident

2024-10-03 | **TLP-CLEAR** | CERT aDvens - CSIRT

Advens - 38 rue des Jeuneurs - 75002 Paris

Sommaire

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

→ La fiche IRM s'adresse aux personnes ou fonctions suivantes :
- Les **RSSI et leurs adjoints**
- Le **CERT**
- Le **SOC**
- Les **administrateurs**

Dans le cas d'un incident : Lire l'IRM et prendre des notes.
Rester calme et contacter immédiatement l'équipe de réponse à incident du secteur d'activité ou un CERT si nécessaire.

Étapes de traitement des incidents

6 étapes sont définies pour gérer les incidents de sécurité :

1. **Préparation** : Se préparer à gérer l'incident,
2. **Identification** : Détecter l'incident,
3. **Confinement** : Limiter l'impact de l'incident,
4. **Remédiation** : Supprimer la menace,
5. **Récupération** : Revenir à un état normal,
6. **Capitalisation et apprentissage** : Élaborer et améliorer les processus.

Cette IRM fournit des informations détaillées pour chaque étape. Les étapes sont issues du **NIST**.

Cette fiche est issue du travail collaboratif avec le **CERT-SG** de modification et de mise à jour de leurs fiches de méthodologie de réponse à incident.

Références

→ IRM CERT-SG
→ IRM CERT-aDvens

1. Préparation

Objectif : Établir des contacts, définir des procédures, recueillir des informations et se familiariser avec les outils de détection d'intrusion pour gagner du temps lors d'une attaque.

- → Avoir des schémas à jour décrivant les composants applicatifs liés au serveur web,
- → S'assurer d'avoir une cartographie des réseaux à jour,
- → Créer un site Web de pré-production prêt à l'emploi, sur lequel il est possible de publier du contenu,
  - Définir une procédure pour rediriger chaque visiteur vers ce site de secours (une page de maintenance statique par exemple),
- → Déploiement d'outils de surveillance et de prévention des intrusions (WAF, fail2ban, etc.) pour détecter et prévenir toute activité anormale ciblant les serveurs Web critiques,
- → Exporter les journaux du serveur Web vers un serveur externe,
  - S'assurer que les horloges sont synchronisées entre chaque serveur (même serveur NTP),
- → Déploiement de règles de détection d'attaques et d'exploitation de vulnérabilités basées sur les journaux du serveur et les surveiller,
- → Auditer les sites web avant la mise à jour et de manière régulière (mensuelle si possible),
- → Référencer toutes les sources de contenus externes statiques ou dynamiques,
- → Avoir à portée de main les contacts opérationnels de l'hébergeur,
- → S'assurer que le fournisseur d'hébergement applique des politiques pour consigner tous les événements et vérifier la conformité contractuelle,
- → Préparer des modèles de communication au cas où l'incident serait visible pour les utilisateurs.

2. Identification

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

Les canaux de détection habituels

- → Surveillance de page Web :
  - Le contenu d'une page Web a été altéré. Le nouveau contenu est soit très discret (une injection « iframe » par exemple) soit explicite (« Vous avez été piraté par xxx »),
- → Utilisateurs :
  - Réception des appels d'utilisateurs ou des notifications d'employés concernant des problèmes qu'ils constatent lors de leur navigation sur le site,
- → Contrôles de sécurité avec des outils tels que Google SafeBrowsing,

Vérifier l'incident de dégradation et détectez son origine

- → Vérifier les métadonnées des fichiers (plus particulièrement : vérifiez les dates de modification, les signatures de hachage),
- → Vérifier les fournisseurs de contenu (mashup),
- → Vérifier les liens présents dans le code source (src, meta, css, scripts …),
- → Vérifier les journaux et les alertes générées par les règles de détection,
- → Analyser les bases de données à la recherche de contenu malveillant.

Le code source de la page suspecte doit être analysé avec soin pour identifier et cerner le problème.
S'assurer que le problème provient d'un serveur Web appartenant à l'entreprise et non du contenu Web situé en dehors de l'infrastructure, comme les bannières publicitaires d'un tiers par exemple.

3. Confinement

Objectif : Atténuer les effets de l'attaque sur l'environnement ciblé.

- → Sauvegarder toutes les données stockées sur le serveur Web à des fins de collecte de preuve et d'investigation :
  - La meilleure pratique, le cas échéant, consiste à créer une copie bit à bit complète du disque dur utilisé par le serveur Web,
  - Cela peut notamment être utile pour récupérer du contenu supprimé.
- → Contrôler l'architecture réseau. Vérifier que la vulnérabilité exploitée par l'attaquant ne se situe pas ailleurs,
  - Vérifier le système sur lequel le serveur Web est exécuté,
  - Vérifier les autres services en cours d'exécution sur cette machine,
  - Vérifier les connexions entrantes et sortantes établies à partir du serveur,

Si la source de l'attaque provient d'un autre système, faire une investigation sur la machine suspecte.

- → Rechercher des preuves derrière chaque action réalisée par l'attaquant :
  - Découvrir comment l'attaquant est entré dans le système en premier lieu et corrigez ce qui peut l'être :
    - → Une vulnérabilité d'un composant Web permettant un accès en écriture : corriger la vulnérabilité en appliquant les correctifs applicables,
    - → Les vulnérabilités des plugins CMS sont souvent exploitées par des attaquants et doivent être identifiées et corrigées,
    - → Au niveau d'un dossier public : le rendre privé,
    - → Faiblesse SQL permettant l'injection : corrigez le code,
    - → Fournisseur de contenu (mashup) : couper les flux impliqués,
    - → Une modification administrative par accès physique : modifier les droits d'accès.

Si nécessaire (problème complexe sur un serveur web important), déploiement d'un serveur web provisoirement à jour.
Le serveur doit proposer le même contenu que celui de la machine compromise ou au moins afficher un contenu légitime tel qu'une page de maintenance statique. Le mieux est d'afficher un contenu statique temporaire, ne contenant que du code HTML.
Cela empêche une autre infection au cas où l'attaquant serait toujours en mesure d'exploiter la même vulnérabilité.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

- → Supprimer tous les contenus modifiés et les remplacer par du contenu légitime, restauré à partir d'une sauvegarde antérieure,
- → S'assurer que ce contenu est exempt de vulnérabilités ; patcher si nécessaire.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

- → Modifier tous les mots de passe utilisateur. Si le serveur Web fournit une authentification utilisateur et qu'il y a des preuves ou des raisons de penser que les mots de passe peuvent avoir été compromis,
  - Cela peut nécessiter une campagne de communication auprès des utilisateurs,
- → Si un serveur de sauvegarde a été utilisé, restaurer les composants du serveur Web principal à l'état nominal,
- → Surveiller de près les journaux et les alertes pour détecter de nouvelles attaques.

6. Capitalisation et apprentissage

Objectif : Documenter les détails de l'incident, discuter des leçons apprises et améliorer les dispositifs et stratégies de défense.

Le rapport d'incident

Il doit être rédigé et mis à la disposition de toutes les parties prenantes de la cellule de gestion de crise.

Le retour d'expérience

Les thèmes du retour d'expérience doivent être décrits avec les éléments suivants :

- → Cause initiale de l'infection,
- → Actions et chronologies de chaque événement important,
- → Ce qui s'est bien passé,
- → Ce qui ne s'est pas bien passé,
- → Coût de l'incident,
- → Indicateurs de compromission.

La capitalisation

Des actions d'amélioration des processus de gestion des incidents doivent être définies pour capitaliser sur cette expérience.