aDvens

Security for the greater good

Attaque réseau

Méthodologie de réponse à incident

IRM-05 | 2022-11-30 | **TLP-CLEAR** | CERT aDvens - CSIRT
Advens - 16 Quai de la Mégisserie - 75001 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.

1.1. Systèmes de détection d'intrusion (EDR, NIPS, IPS)

- S'assurer que les outils de surveillance sont à jour,
- Établir une liste des contacts avec les équipes d'exploitation de réseau et de sécurité,
- S'assurer qu'un processus de notification d'alerte est défini et bien connu de tous,
- Vérifier l'accès à l'appareil et sa capacité à surveiller les périmètres concernés,
- S'assurer qu'il est possible d'isoler les terminaux ou stations de travail, ou la zone (à l'aide d'un EDR par exemple ou par un pare-feu).

1.2. Réseau

- S'assurer qu'un inventaire des points d'accès au réseau est disponible, accessible et à jour, si possible avec un suivi des différentes versions du document,
- S'assurer que les équipes réseau disposent d'une cartographie et des configurations réseau à jour avec les zones et les équipes opérationnelles concernées,
- Rechercher régulièrement les points d'accès réseau potentiellement indésirables et les fermer,
- Rechercher un accès VPN et/ou un accès Cloud depuis des adresses ou des localisations rares,
- Déployer et surveiller les outils de gestion du trafic.

1.3. Trafic de base

- Identifier le trafic et les flux de référence,
- Identifier les flux critiques pour l'entreprise.

S'assurer que les équipes connaissent les outils et sachent les utiliser.
Garder les journaux opérationnels même lorsqu'ils ont été archivés.
Avoir une bonne politique de conservation des logs est indispensable (plus de 6 mois).

2. Identification

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

2.1. Sources de détection

- Notification par les utilisateurs / support utilisateur (helpdesk),
- Journaux, alertes et rapports IDS/IPS/NIDS/EDR,
- Détection par l'équipe réseau,
- Journaux du pare-feu et du proxy,
- Plainte provenant d'une source externe,
- Honeypots ou toute autre solution de déception.

2.2. Enregistrer l'activité réseau suspecte

- Les trames réseau peuvent être stockées dans un fichier et transmises à l'équipe de réponse aux incidents pour une analyse plus approfondie,
- Utiliser des outils de capture réseau (tshark, windump, tcpdump ...) pour collecter le trafic malveillant,
- Utiliser un concentrateur ou des ports en miroir sur un réseau local infecté pour collecter les données,
- L'investigation réseau nécessite des compétences et des connaissances. Demander de l'aide ou des conseils à l'équipe d'intervention en cas d'incident,
- Savoir restaurer et consulter les logs même lorsqu'ils ont été archivés.

2.3. Analyser l'attaque

- Analyser les alertes générées par l'IDS,
- Consulter les statistiques et les journaux des périphériques réseau,
- Essayer de comprendre l'objectif du trafic malveillant et d'identifier les composants de l'infrastructure affectés par celui-ci,
- Cartographier avec les risques business pour hiérarchiser correctement l'analyse ou le confinement,
- Identifier les caractéristiques techniques du trafic :
  - Adresse(s) IP source(s),
  - Ports utilisés, TTL, Packet ID, ...
  - Protocoles utilisés,
  - Machines et/ou services ciblés,
  - Exploit(s) utilisé(s),
  - Comptes distants connectés.

A l'issue de cette étape, les machines impactées et le modus operandi de l'attaque doivent avoir été identifiés.
Idéalement, la source de l'attaque aurait également dû être identifiée. C'est là que débute l'investigation, si nécessaire.
Si un ordinateur compromis a été identifié, consulter les IRM dédiées à l'intrusion, IRM-02 pour Windows et IRM-03 pour Linux.

3. Confinement

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

Si l'incident est considéré comme stratégique (accès aux ressources sensibles), une cellule de gestion de crise spécifique doit être activée.

En fonction de la criticité des ressources impactées, les étapes suivantes peuvent être réalisées et surveillées :

- → Déconnecter la zone compromise du réseau,
- → Isoler la source de l'attaque. Déconnecter le ou les ordinateurs concernés afin d'effectuer une investigation numérique,
- → Adopter des contrôles d'atténuation acceptables (MFA, géo-filtrage) pour le flux critique pour l'entreprise en accord avec les responsables métiers,
- → Mettre fin aux connexions ou aux processus indésirables sur les machines concernées,
- → Utiliser les règles de pare-feu, IPS et/ou EDR pour bloquer l'attaque,
- → Utiliser les règles IDS pour faire face à ce comportement malveillant et informer le personnel technique des nouveaux événements,
- → Appliquer des actions spécifiques en cas d'enjeu stratégique :
  - Refuser les connexions externes dans EDR, les proxys et/ou les pare-feux,
  - Configurer la gestion des politiques de contrôle de sécurité pour contenir ou rejeter les connexions des machines compromises,
  - Limiter l'accès aux données critiques/confidentielles,
  - Créer des documents piégés avec des filigranes qui pourraient être utilisés comme preuve de vol,
  - Informer les utilisateurs professionnels ciblés de ce qui doit être fait et de ce qui est interdit,
  - Configurer les fonctionnalités de journalisation en mode détaillé sur l'environnement ciblé et les stocker sur un serveur sécurisé distant.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

4.1. Bloquer la source

- → À l'aide de l'analyse des étapes précédentes d'identification et de confinement, découvrir tous les canaux de communication utilisés par l'attaquant et les bloquer sur toutes les éléments du réseau,
- → Si la source a été identifiée comme un employé, prendre les mesures appropriées et impliquer la direction et/ou l'équipe RH et/ou l'équipe juridique,
- → Si la source a été identifiée comme un attaquant externe, envisager d'impliquer les équipes d'abus identifiées et les forces de l'ordre, si nécessaire.

4.2. Remédiation technique

- → Définir un processus de remédiation. Si nécessaire, ce processus peut être validé par une autre structure, comme l'équipe de réponse aux incidents par exemple,
- → Les étapes de correction des IRM d'intrusion (IRM-2 pour Windows et IRM-3 pour Linux) peuvent également être utiles.

4.3. Tester et appliquer

- → Tester le processus de correction et s'assurer qu'il fonctionne correctement sans endommager aucun service,
- → Appliquer le processus de correction une fois que les tests ont été approuvés par le service informatique et les équipes métiers.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

- → S'assurer que le trafic réseau est revenu à la normale,
- → Autoriser de nouveau les connexions aux segments de réseau précédemment contenus.

Toutes ces étapes doivent être réalisées les uns après les autres avec un suivi technique.

6. Capitalisation et apprentissage

Objectif : Documenter les détails de l'incident, discuter des leçons apprises et ajuster/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.

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 détection des logiciels malveillants et des intrusions sur le réseau doivent être définies pour capitaliser sur cette expérience.