aDvens

Security for the greater good

Compromission d'un tiers

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 pour gagner du temps lors d'une attaque.

- Maintenir un inventaire à jour de tous les tiers, partenaires, fournisseurs et sous-traitants ayant accès aux systèmes, aux données, à l'équipement ou à l'infrastructure de l'organisation.
- Préparer et disposer d'une liste des points de contact facilement accessible des personnes à impliquer dans les contrats de prestation de services avec des tiers.
- Définir des points de contact spécifiques 24 heures sur 24 et 7 jours sur 7, ainsi que des personnes chargées d'intervenir en dehors des heures de travail.
- Mettre en place un processus d'évaluation de la maturité du système d'information des fournisseurs de services intégrés via un questionnaire KYS (*Know Your Supplier*).
- Établir et maintenir des accords de niveau de service (SLA) avec les tiers, y compris des exigences en matière de sécurité et de réponse aux incidents, ainsi que des clauses d'alerte spécifiques en cas de compromission d'un tiers.
- Examiner et évaluer régulièrement les contrôles, les politiques et les procédures de sécurité des tiers.
- Établir une cartographie formelle des interconnexions réseau et des flux de communication applicatifs avec les fournisseurs de services.
- Mettre en place un "*bouton rouge*" pour couper tous les liens informatiques avec le fournisseur de services concerné en cas de nécessité.
- Évaluer la faisabilité, la capacité et le temps nécessaire pour bloquer les liens d'interconnexion avec un tiers ou les accès de tiers; valider par des tests et des exercices de coupure. **Prendre en compte l'impact sur l'entreprise et les exigences des régulateurs.**
- Mener régulièrement des exercices conjoints de réponse aux incidents avec les tiers critiques.
- Préparer une stratégie de communication interne et externe en cas d'incident, y compris des canaux de communication alternatifs pour les contacts concernés.
- Mettre en place un processus de surveillance des blogs et des sites de rançongiciel; dresser une liste complète de mots clés, de catégories industrielles ou de zones géographiques à appliquer au processus de surveillance souhaité. Noter que selon le pays, les activités de recherche impliquant des fuites de données peuvent être soumises à la conformité aux réglementations locales en matière de données, y compris le RGPD et le code pénal.
- Surveiller régulièrement les entreprises qui subissent une cyberattaque, en particulier celles qui sont compromises par un rançongiciel.
- Automatiser les alertes internes pour signaler la présence d'un partenaire sur l'un des sites de blogs en surveillance.
- Préparer des installations dédiées à l'analyse ou à l'isolement par la mise en bac à sable des données et des fichiers concernés à exploiter pendant l'incident.

D'autres exigences légales sont à prendre en compte lors de la mise en place du processus de suivi exemple CNIL RIFI

2. Identification

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

Il peut être nécessaire d'informer les parties prenantes, les partenaires et les autorités de réglementation au début de cette étape le cas échéant.

Détection

- Utiliser une surveillance proactive à partir de la veille des blogs de publication de fuites d'information, de sources ouvertes ou de notifications privées : vérifier et analyser régulièrement tous les flux de renseignement sur les menaces applicables pour détecter rapidement des informations sur les compromissions potentielles de tiers.
- Surveiller en permanence les flux d'entrée et de sortie du réseau pour détecter à temps les anomalies dans les interconnexions avec des tiers.
- Impliquer toutes les parties prenantes identifiées précédemment (entreprise, achats, service juridique, infrastructure, sécurité de l'information, etc.); évaluer l'impact potentiel sur la base des informations disponibles sur l'incident et du retour d'information de l'entreprise et du service informatique.
- Évaluer les scénarios de remédiation possibles : blocage des interconnexions, renforcement de la surveillance en fonction de l'évaluation des risques par rapport à l'impact potentiel sur la production.
- Communiquer l'incident aux niveaux supérieurs de votre organisation (jusqu'au conseil d'administration) afin d'avoir la vision de la situation la plus complète et la plus détaillée.
- Établir des canaux de communication avec les tiers concernés afin de partager des informations sur l'incident en cours. Si la nature de l'incident l'exige, mettre en place d'autres canaux dédiés (hors entreprise) pour la communication et les échanges de données.
- Évaluer le niveau de confiance à accorder au tiers en fonction du niveau de transparence ressenti dans la qualité de sa communication et de la remise effective des rapports d'enquête et de traitement de l'incident applicables, des IOCs, etc.

Recommandations supplémentaires : en cas de signes de latéralisation, merci de vous référer à l'**IRM-18**, Compromission large périmètre.

3. Confinement

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

Si l'incident implique l'accès à des ressources sensibles de l'organisation, une cellule de gestion de crise spécifique peut être convoquée.

- → Suspendre temporairement ou restreindre l'accès du tiers concerné aux systèmes, données, équipements ou infrastructures de l'organisation, si nécessaire.
- → Limiter complètement ou partiellement la communication par e-mail (en redirigeant les courriels échangés vers un environnement ou une boîte aux lettres dédiée, en supprimant les pièces jointes, les liens ou tout autre contenu).
- → Organiser des réunions régulières avec le fournisseur concerné, en intégrant les parties prenantes concernées.
- → Coordonner avec le tiers concerné la mise en œuvre de mesures de confinement, telles que l'isolement des systèmes compromis, le blocage des IOC malveillants ou la réinitialisation des identifiants.

Si cela s'applique aux IOC obtenus:

- → Bloquer le trafic vers les C&C.
- → Bloquer toute IP détectée comme étant utilisée par les attaquants.
- → Désactiver les comptes compromis/créés par les attaquants.
- → Envoyez les échantillons non détectés à votre fournisseur de sécurité des points finaux et/ou à des bacs à sable privés d'analyse de code malveillant.
- → Envoyer les IP, URL et noms de domaine malveillants inconnus à votre fournisseur de sécurité périmétrique.

Si le trafic critique pour l'entreprise ne peut pas être déconnecté, autoriser-le après avoir mis en place des contrôles de sécurité supplémentaires afin de détecter et de limiter ou d'empêcher une possible latéralisation.

4. Remédiation

Objectif : Prendre des mesures pour limiter l'impact sur la production.

- → Réévaluer la transparence et la mise en oeuvre des efforts de remédiation du tiers.
- → Envisager de demander un rapport d'incident formel dans le cadre du processus de traitement de l'incident ou d'une enquête judiciaire, c'est-à-dire une lettre d'engagement signée par le conseil d'administration du fournisseur ou un rapport d'investigation du prestataire de réponse à incident ou du service judiciaire en charge de l'incident.
- → Demander une liste actualisée des IOCs détectés, ceux identifiés durant et par le processus d'investigation.

5. Récupération

Objectif : Restaurer le fonctionnement initial du système.

Toutes les étapes suivantes doivent être réalisées de manière progressive et avec un suivi technique.

- → Obtenir un rapport formel d'un tiers de confiance garantissant que la situation du demandeur est effectivement revenue à la normale.
- → Décider avec les acteurs identifiés en interne si la réouverture des services et des interconnexions avec le partenaire est possible.
- → Collaborer avec le tiers concerné pour rétablir les services ou les systèmes affectés, en veillant à ce qu'ils soient sécurisés et exempts de vulnérabilités connues.
- → Réévaluer et mettre à jour le profil de risque du tiers à la lumière de l'incident.
- → Rétablir progressivement l'accès du tiers aux systèmes, aux données et à l'infrastructure de votre organisation, en s'assurant que les mesures de sécurité appropriées sont en place.

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.