aDvens

Security for the greater good

Fuite de données

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.

1.1. Contacts

- Identifier les contacts techniques internes (équipe de sécurité, équipe de réponse aux incidents…),
- S'assurer d'avoir des points de contact dans l'équipe de relations publiques (institutions de régulation), l'équipe de ressources humaines et le service juridique,
- Identifier les contacts externes qui pourraient être nécessaires, principalement à des fins d'enquête (comme les forces de l'ordre par exemple),
- Préparer la stratégie de communication interne et externe,
- Maintenir la liste de contacts DPO, DT et RGPD.

1.2. Politique de sécurité

- S'assurer que la valeur des informations de l'entreprise est expliquée dans le règlement intérieur, la charte informatique, la session de sensibilisation et de formation,
- S'assurer que tous les actifs de valeur sont identifiés comme il se doit,
- S'assurer que le processus d'escalade des incidents de sécurité est défini et que les acteurs sont clairement identifiés.

2. Identification

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

La fuite de données peut se produire de n'importe où.
Ne pas oublier que la cause de la fuite peut être un employé qui contourne volontairement ou non les problèmes de sécurité, ou un ordinateur compromis (c'est-à-dire une attaque à grande échelle / rançongiciel).

2.1. Détection de la fuite

Processus de notification d'incident

- → Les informations internes peuvent être une bonne source de détection : employés de confiance, équipe de sécurité identifiant un problème …,

Outil de veille publique

- → Une veille sur les moteurs de recherche Internet et les bases de données publiques peut être très précieuse pour détecter les fuites d'informations,
- → Surveiller les sites de publication de rançongiciels pour détecter les fuites de données potentielles, y compris celles de tiers.

Outil de DLP (prévention des pertes de données)

- → S'il existe un outil de DLP dans l'entreprise, il peut fournir des informations précieuses aux gestionnaires d'incidents travaillant sur les fuites d'informations.

2.2. Confirmer l'incident

Ne rien faire sans une demande écrite du RSSI/responsable concerné.
Sur la base des conseils de l'équipe juridique, une autorisation écrite de l'utilisateur concerné peut également être utile.

Courriel

- → La source de divulgation pourrait avoir envoyé des données en utilisant son adresse e-mail professionnelle,
- → Sur le système de messagerie, rechercher les e-mails envoyés ou reçus d'un compte suspect ou avec un sujet spécial,
- → Sur le client de messagerie sur le bureau du suspect (si disponible), utiliser un outil qui permet de rechercher en filtrant les e-mails marqués « PRIVÉ », si besoin, demander à l'utilisateur un accord écrit ou lui demander d'être présent,
- → Le cas échéant, consultez les journaux associés.

Navigation

- → Des données peuvent avoir été envoyées sur des webmails/forums/sites dédiés.
- → Sur le serveur proxy ou SIEM, vérifier les journaux relatifs aux connexions du compte suspect sur l'URL suspecte utilisée pour divulguer des données,
- → Sur le bureau (si disponible), vérifier l'historique des navigateurs installés. Ne pas oublier que certaines personnes peuvent avoir différents navigateurs sur le même ordinateur de bureau,
- → Vérifier l'historique de tous les navigateurs du poste,
- → Si le moment de la fuite de données a été horodaté, certains journaux peuvent fournir des informations utiles.

Périphériques de stockage externes

- → De nombreux supports peuvent être utilisés pour stocker des données : clés USB, CD-ROM, DVD, disques durs externes, smartphones, cartes mémoire …,
- → Peu d'informations seront trouvées concernant le transfert de données à l'aide de ces appareils,
- → La clé USB utilisée pour transférer les données peut être référencée par le système d'exploitation,
- → Une investigation peut confirmer l'utilisation du matériel mais pas forcément les données transmises.

Fichiers locaux

→ Si rien n'a encore été trouvé, il est possible de retrouver des traces dans le système de fichiers local du suspect, tout comme pour les recherches de courriel, utiliser un outil de collecte qui interdit tout accès à la zone PRIVÉE de l'utilisateur.

→ Si besoin, agir conformément au droit du travail.

Transfert réseau

Plusieurs moyens peuvent être utilisés pour transférer des données hors de l'entreprise :

→ FTP, messagerie instantanée, etc. Essayer de creuser dans les journaux indiquant une telle activité.

→ Les données peuvent également avoir été envoyées via un tunnel VPN ou sur un serveur SSH.

- Dans ce cas, la connexion peut être découverte en regardant les journaux mais le contenu transmis rarement.

Imprimante

→ Les données peuvent être envoyées aux imprimantes connectées au réseau. Dans ce cas, vérifier les traces sur le spooler ou directement sur l'imprimante, car certains constructeurs stockent directement les documents imprimés sur un disque dur local.

Logiciels malveillants/ransomware

→ Une compromission malware/ransomware peut être à l'origine d'une fuite d'informations et doit être traitée en conséquence avec **l'IRM-07 « Détection de malware » ou « Rançongiciel » IRM-17**.

Même lorsque suffisamment de preuves ont été trouvées, chercher toujours plus.
Ce n'est pas parce qu'il y a une preuve que des données sont passées frauduleusement de A à B avec une méthode qu'elles n'ont pas été également envoyées à C avec une autre méthode. Ne pas oublier non plus que quelqu'un d'autre aurait pu accéder à l'ordinateur.
L'employé suspect était-il réellement devant son ordinateur lorsque la fuite s'est produite ?

2.3. Analyser les données concernées si disponibles

Parfois, les données divulguées peuvent être téléchargées et analysées par l'équipe de sécurité.
Les groupes de rançongiciel publient souvent des informations divulguées sur leur site dédié.
L'utilisation d'outils d'analyse de données comme Aleph ou d'autre peut aider les équipes juridiques à décider des mesures à prendre.

À la fin de cette phase, il peut être envisager d'impliquer les forces de l'ordre et les régulateurs si nécessaire.

3. Confinement

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

- → Informer les manager, l'équipe juridique et l'équipe des relations publiques/communication pour s'assurer qu'ils sont prêts à faire face à une divulgation massive ou ciblée,
- → Selon le vecteur de fuite, bloquer l'accès à l'URI de divulgation, au serveur de divulgation, à la source de divulgation ou aux destinataires de la divulgation,
  - Cette action doit être effectuée sur tous les points de l'infrastructure.
- → Suspendre les identifiants de connexion logiques et physiques de l'employé suspect, si la fuite a été confirmée :
  - Impliquer l'équipe RH et juridique avant toute action.
- → Isoler le système informatique (ordinateur de bureau, imprimante) utilisé pour divulguer les données afin d'effectuer une investigation forensique ultérieurement,
  - Cette manipulation doit être faite brutalement : retirer la prise électrique (et la batterie dans le cas d'un ordinateur portable).

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

- → Si des données ont été envoyées à des serveurs publics :
  - Demander au propriétaire (ou au webmaster) de supprimer les données divulguées,
  - Veiller à bien adapter la demande aux destinataires (le webmaster hacktiviste ne se comportera pas comme un webmaster journaliste).
- → S'il n'est pas possible de supprimer les données divulguées :
  - Fournir une analyse complète à l'équipe des relations publiques et à la direction.
  - Surveiller les documents divulgués sur les sites Web et les réseaux sociaux (FB, Twitter, etc.) et les commentaires ou réactions des internautes.

Fournir les éléments à l'équipe RH pour éventuellement porter plainte contre l'employé.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

- → Si un système a été compromis, le restaurer complètement,
- → Avertir éventuellement les collaborateurs ou certaines équipes locales du problème pour les sensibiliser et renforcer les règles de sécurité,
- → Lorsque la situation revient à la normale, la communication officielle pourrait être supprimée.

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.