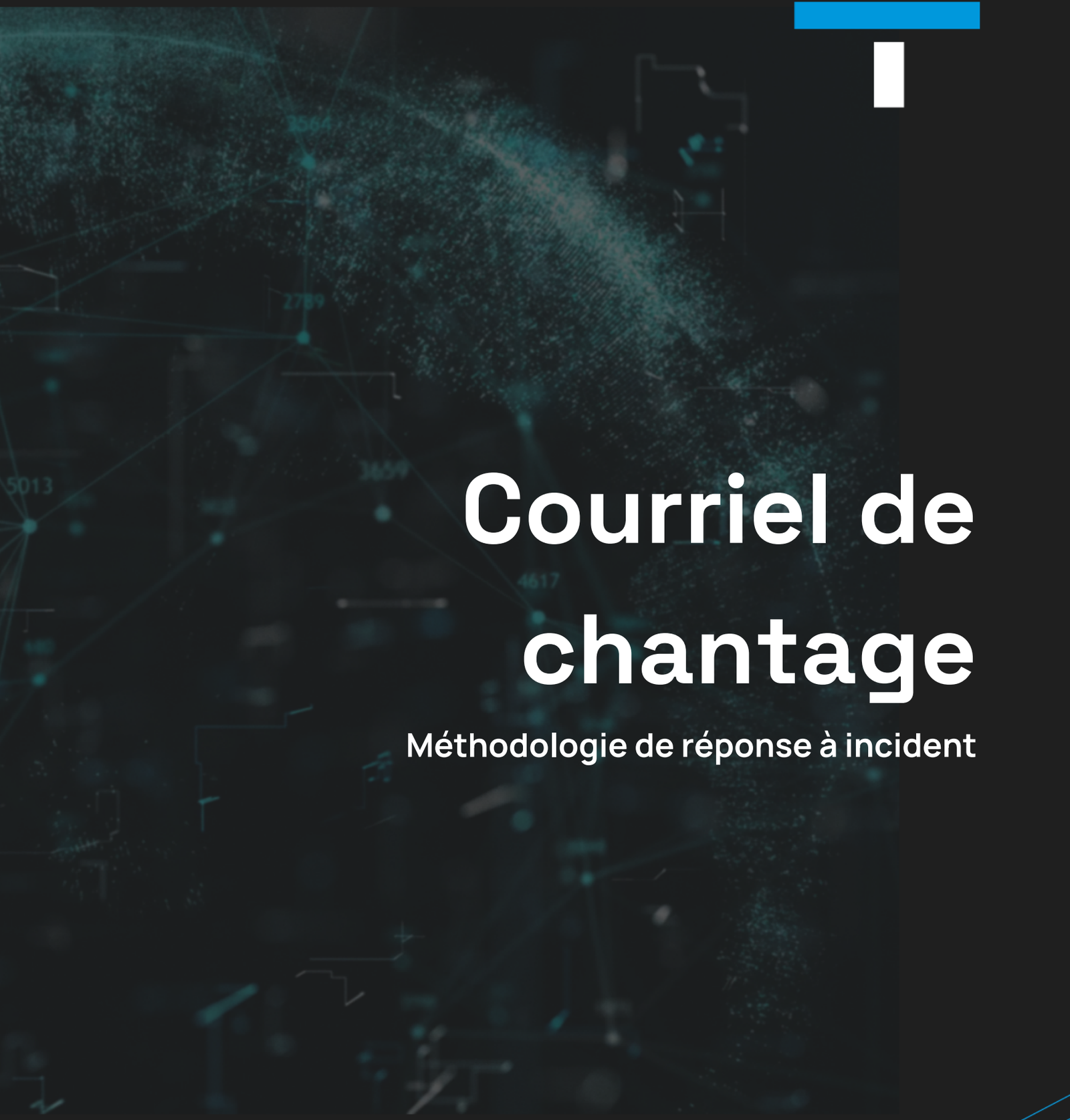
aDvens

Security for the greater good



Courriel de chantage

Méthodologie de réponse à incident

IRM-08 | 2022-11-30 | **TLP-CLEAR** | CERT aDvens - CSIRT
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

INTRODUCTION 2
ÉTAPES DE TRAITEMENT DES INCIDENTS 2
1. PRÉPARATION 3
1.1. Contacts 3
1.2. Sensibilisation 3
2. IDENTIFICATION 4
3. CONFINEMENT 5
4. REMÉDIATION 6
5. RÉCUPÉRATION 6
6. CAPITALISATION ET APPRENTISSAGE 6

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 internes (équipe de sécurité, équipe de réponse aux incidents, service juridique, etc.),
- Identifier les contacts externes qui pourraient être nécessaires, principalement à des fins d'enquête comme les forces de l'ordre,
- S'assurer que le processus d'escalade des incidents de sécurité est défini et que les acteurs sont clairement identifiés,
- S'assurer d'avoir des capacités de collecte de renseignements (communautés, contact, etc.) qui pourraient être impliquées dans de tels incidents.

1.2. Sensibilisation

- S'assurer que tous les employés concernés sont conscients des problèmes de chantage. Le programme de sensibilisation à la sécurité peut l'inclure.

Vérifier que le processus de sauvegarde et de réponse aux incidents est en place et à jour.

2. Identification

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

- Alerter les personnes concernées,
- Garder des traces de toutes les communications liées à l'incident,
  - Ne pas supprimer de courriel; noter tout contact téléphonique avec numéro de téléphone et horodatage si possible,
  - Essayer d'obtenir autant de détails que possible sur l'auteur (nom , fax, adresse postale, etc.).
- Envisager les actions possibles avec l'équipe de réponse aux incidents et l'équipe juridique,
- Analyser les e-mails pour obtenir toutes les informations sur l'incident (nom d'utilisateur, serveurs MX, …),
- S'il s'agit de données internes, vérifier la présence d'une sauvegarde sécurisée et essayer de savoir comment elles ont été collectées,
- Inclure la direction pour les informer qu'un chantage se produit et est traité selon le processus défini.

3. Confinement

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

→ Déterminer comment répondre au chantage avec les conséquences et les coûts s'il est ignoré, répondre si oui ou non.

Les menaces les plus courantes liées au chantage sont

→ Déni de service
→ Révéler des données sensibles sur Internet (carte de crédit ou autres données personnelles de clients ou d'un employé/directeur interne, données confidentielles de l'entreprise, etc.),
→ Révéler des informations privées sensibles sur les employés/VIP,
→ Bloquer l'accès aux données (effacées ou chiffrées via un rançongiciel par exemple),
→ Envoi massif utilisant la marque (spam, sextorsion, pédopornographie, mauvaises rumeurs, etc.).

Vérifier l'arrière-plan

→ Vérifiez si des tentatives de chantage similaires ont eu lieu dans le passé. Vérifier si d'autres entreprises ont également été menacées,
→ Toutes les données techniques connexes doivent être soigneusement vérifiées et collectées à des fins d'investigation,
→ Rechercher si quelqu'un aurait intérêt à menacer votre entreprise :
  - Concurrents,
  - Groupes à motivation idéologique,
  - Employés anciens ou actuels.
→ Essayer d'identifier l'attaquant avec les informations disponibles,
→ Plus généralement, **essayer de trouver comment l'attaquant est entré dans le système ou a obtenu l'objet du chantage.**

→ Contacter les forces de l'ordre locales pour les informer.

Essayer de gagner du temps et des détails auprès du fraudeur. Demander

→ Une preuve de ce qu'il dit : exemple de données, preuve d'intrusion, etc,
→ Gagner du temps pour obtenir ce que veut le fraudeur (argent, etc.).

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

Si une faille a été identifiée sur un bien technique ou un procédé permettant à l'attaquant d'accéder à l'objet du chantage, demander une correction **IMMÉDIATE** afin d'éviter un autre cas.

- → Après avoir obtenu autant d'informations que possible, ignorer le chantage et s'assurer qu'une surveillance appropriée est en place pour détecter et réagir en conséquence avec un nouveau suivi,
- → Ne prendre aucune décision de remédiation seul si des actifs stratégiques ou des personnes sont ciblés. Impliquer les départements ou les métiers appropriés.

Une réponse positive au fraudeur est une porte ouverte pour d'autres chantages.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Informer la direction des actions et de la décision prises sur le cas de chantage.

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.