aDvens

Security for the greater good

Attaque par ingénierie sociale

Méthodologie de réponse à incident

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

Advens - 38 rue des Jeuneurs - 75002 Paris

Sommaire

INTRODUCTION 2
ÉTAPES DE TRAITEMENT DES INCIDENTS 2
1. PRÉPARATION 3
2. IDENTIFICATION 4
2.1. Appel téléphonique 4
2.2. E-mail 4
3. CONFINEMENT 5
3.1. Actions pour tous les employés 5
3.2. Actions pour le CERT ou l'équipe de réponse à incident 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.

→ Sensibiliser les utilisateurs sur les politiques de sécurité.

Ne jamais donner de renseignements personnels ou sur l'entreprise à une personne non identifiée.
Cela peut inclure les identifiants d'utilisateur, les mots de passe, les informations de compte, le nom, l'adresse e-mail, les numéros de téléphone (mobile ou fixe), l'adresse, le numéro de sécurité sociale, les intitulés de poste, des informations sur les clients, l'organisation ou les systèmes informatiques.
Le but de l'ingénierie sociale est de voler des ressources humaines, des secrets d'entreprise ou des données client / utilisateur.

→ Signaler tout événement suspect à votre responsable, qui le transmettra au RSSI afin d'avoir un reporting centralisé,
- Avoir un processus défini pour rediriger toute demande "étrange" vers un téléphone "rouge", si nécessaire,
- Se préparer à gérer la conversation avec les arnaqueurs pour identifier les informations qui pourraient aider à suivre l'attaquant et ses objectifs,
- Consulter le service juridique pour voir quelles actions sont autorisées et quelles réactions ils peuvent gérer.

Téléphone rouge :
Le numéro de téléphone rouge doit être clairement identifié comme "Ingénierie sociale".
Le numéro de téléphone doit être facile à identifier dans l'annuaire téléphonique global de l'entreprise mais les demandes au numéro ne doivent pas être affichées.
La ligne du téléphone rouge doit toujours être enregistrée dans le but de collecter des preuves.

2. Identification

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

2.1. Appel téléphonique

Un inconnu appelle un service, demandant des informations détaillées.

- Si le contact travaille en dehors de l'entreprise et demande des informations qui pourraient être précieuses pour un concurrent, refuser ses demandes et passer à la partie 3,
- Si le contact se fait passer pour un employé de l'entreprise mais que le numéro de téléphone est masqué ou non interne, lui proposer de rappeler le numéro déclaré dans l'annuaire,
- Si l'agresseur supposé est d'accord, le rappeler pour vérifier. S'il refuse cette option, passer à la partie 3.

L'attaquant peut utiliser plusieurs techniques pour inciter sa victime à parler (peur, curiosité, empathie …). Ne divulguer en aucun cas des informations.

- **Écouter attentivement ses demandes et demander à la fin un numéro de téléphone pour rappeler ou une adresse e-mail pour répondre,**
- **Prendre des notes et rester calme, même si l'agresseur crie ou menace, se rappeler qu'il essaie d'utiliser les faiblesses humaines.**

Pour aller plus loin, les informations suivantes seront précieuses :

- Le nom du correspondant,
- Informations / personnes demandées
- Accent, compétences linguistiques,
- La langue de l'appelant et les connaissances organisationnelles,
- Bruits de fond / environnement,
- Heure et durée de l'appel.

2.2. E-mail

Un inconnu demande des informations détaillées.

- Si le contact a une adresse e-mail "hors de l'entreprise" et demande des informations qui pourraient être précieuses pour un concurrent, passer à la partie 3,
- Si le contact utilise une adresse e-mail interne mais demande des informations bizarres, lui demander quelques explications et utiliser l'annuaire de l'entreprise pour obtenir le nom de son responsable pour le placer en copie,
- Avertir éventuellement la direction pour l'informer qu'un incident lié à une attaque d'ingénierie sociale a été rencontré. Ils pourraient comprendre les objectifs en fonction du contexte.

3. Confinement

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

3.1. Actions pour tous les employés

Appel téléphonique

- → Si l'attaquant demande instamment de donner un numéro de téléphone, suivre ces étapes:
  - Utiliser la "ligne téléphonique rouge" du CERT/CSIRT, si elle existe,
  - Lui donner le numéro avec un nom inventé,
  - Appeler immédiatement l'équipe CERT/CSIRT en expliquant ce qui s'est passé et le nom inventé choisi.
- → Si l'agresseur stresse trop et ne laisse pas le temps de trouver le numéro de téléphone rouge, lui demander de rappeler plus tard, en faisant semblant d'avoir un rendez-vous.
- → Si l'attaquant veut atteindre quelqu'un, suivre ces points :
  - Mettre en attente l'attaquant et appeler l'équipe CERT/CSIRT et expliquer ce qui s'est passé,
  - Transférer la conversation de l'attaquant à l'équipe CERT/CSIRT (**ne pas lui donner le numéro**).

Courriel

- → Transférer à l'équipe de sécurité tous les e-mails, y compris les en-têtes (à envoyer en pièces jointes) à des fins d'enquête. Cela pourrait aider à suivre l'attaquant.

3.2. Actions pour le CERT ou l'équipe de réponse à incident

Appel téléphonique

- → Résumer la conversation téléphonique avec l'attaquant en utilisant les techniques suivantes :
  - Anonymiser l'identité de la personne qui va parler avec l'arnaqueur,
  - Calmer la conversation pour la faire durée et pousser à la faute l'attaquant,
  - Lui expliquer que les attaques par ingénierie sociale sont strictement interdite par la loi, que c'est répréhensible et que l'équipe juridique continuera l'incident s'il ne s'arrêt pas.
- → *Si le téléphone rouge a été utilisé, préparer sa destruction et la création d'un nouveau.*

Courriel

- → Collecter le maximum d'information possible sur l'adresse de courriel,
- → Analyser les entêtes des messages et essayer de localiser l'émetteur,
- → Rechercher l'adresse émettrice avec des outils sur Internet,
- → Géolocaliser, si possible, l'utilisateur derrière l'adresse de courriel.

Agréger toutes les attaques par ingénierie sociale pour en visualiser le schéma.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

Certaines actions correctives possibles peuvent être tentées

- → Alerter les forces de l'ordre et/ou porter plainte,
- → Discuter du problème dans les cercles de confiance pour savoir si l'entreprise est seule face à ce problème,
- → Menacer l'agresseur de poursuites judiciaires s'il peut être identifié,
- → Signaler les adresses e-mail utilisées par l'attaquant aux équipes de sécurité du fournisseur.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Notifier au top management les actions et les décisions prises sur le cas d'ingénierie sociale.

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.