aDvens

Security for the greater good

Hameçonnage de clients

Méthodologie de réponse à incident

IRM-13 | 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.

- → Créer une liste de tous les domaines légitimes appartenant à l'entreprise. Cela aidera à analyser la situation et évitera de lancer une procédure de retrait sur un site Web légitime oublié,
- → Préparer une page Web hébergée sur l'infrastructure, prête à être publiée à tout moment, pour avertir les clients d'une attaque de phishing en cours,
  - Préparer et tester également une procédure de déploiement.
- → Préparer des modèles de demande de retrait des sites par courriel,
  - Ils seront utilisés pour chaque cas de phishing, si possible, en plusieurs langues. Cela accélérera les choses lorsque une tentative de joindre la société d'hébergement sera effectuée, etc. pendant le processus de retrait.
- → Déployer DKIM, DMARC et SPF sur toute la chaîne de messagerie,
- → Surveiller les domaines typosquattés et le contenu qui y est publié,
  - Rassembler les informations de contact et d'abus au cas où.

1.1. Interlocuteurs internes

- → Maintenir une liste de toutes les personnes impliquées dans l'enregistrement des noms de domaine dans l'entreprise,
- → Maintenir une liste de toutes les personnes accréditées pour prendre des décisions sur la cybercriminalité et les actions éventuelles concernant le phishing.
  - Si possible, obtenir un accord écrit qui permettant à l'intervenant de prendre ce genre de décisions.

1.2. Interlocuteurs externes

- → Avoir plusieurs moyens pour être joint à temps (24/7 si possible) :
  - Adresse e-mail facile à retenir pour tous (ex : sécurité@entreprise),
  - Formulaires Web sur le site Web de l'entreprise (l'emplacement du formulaire est important, pas plus de 2 clics de la page principale),
  - Compte Twitter visible,
- → Établir et tenir à jour une liste de contacts de retrait dans :
  - Sociétés d'hébergement,
  - Sociétés d'enregistrement,
  - Fournisseurs de messagerie.
- → Établir et maintenir des contacts avec des CERT à travers le monde qui pourraient être en mesure d'apporter leur aide.

1.3. Sensibiliser les clients

Ne pas attendre les incidents de phishing pour communiquer avec les clients.

- → Sensibiliser à la fraude par phishing,
  - Expliquer ce qu'est le phishing et s'assurer que les clients savent qu'aucune demande d'informations d'identification/bancaires par e-mail ou par téléphone ne leur sera demandée.

1.4. Sensibiliser les métiers

Les personnes des métiers doivent être conscientes des problèmes de phishing et considérer la sécurité comme une priorité.
Par conséquent, ils doivent appliquer de bonnes pratiques telles qu'éviter d'envoyer des liens (URL) aux clients et utiliser une signature indiquant que l'entreprise ne leur demandera jamais d'informations d'identification/bancaires en ligne.

2. Identification

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

2.1. Détection d'hameçonnage

- → Surveiller de près tous les points de contact (e-mail, formulaires web, etc.),
- → Déployer des pièges à spam et collecte des spams de partenaires/tiers,
- → Déployer une surveillance active des référentiels de phishing, comme PhishTank et Google Safe Browsing par exemple,
- → Surveiller de toutes les listes de diffusion spécialisée ou tous flux RSS/Twitter, qui pourraient signaler des cas de phishing,
- → Utiliser des systèmes de surveillance automatisés sur toutes ces sources, afin que chaque détection déclenche une alarme pour une réaction instantanée,
- → Surveiller les journaux Web. Vérifier qu'aucune redirection suspecte n'amène des personnes sur un site Web malveillant. Les utilisateurs sont souvent redirigés depuis le site malveillant vers le site légitime après la récupération des identifiants.

2.2. Appliquer le bon processus

- → Dès qu'un site de phishing est détecté, contacter les personnes de l'entreprise habilitées à prendre une décision,
- → La décision d'agir sur le site/l'adresse e-mail frauduleux doit être prise dans les meilleurs délais, en quelques minutes.

2.3. Recueillir des preuves

- → Faire une copie horodatée des pages Web de phishing,
  - Utiliser un outil efficace pour le faire, comme HTTrack par exemple,
  - Ne pas oublier de prendre toutes les pages du site de phishing, pas seulement la première s'il y en a plusieurs,
  - Si nécessaire, faire des captures d'écran des pages.
- → Vérifiez le code source du site Web de phishing :
  - Voir où les données sont exportées : soit vers un autre contenu web pour lequel l'accès n'est pas possible (un script PHP généralement), envoyé par e-mail au fraudeur ou via une API d'application (comme Telegram par exemple),
  - Rassembler des informations sur l'acteur de phishing qui peuvent être disponibles dans l'URI, le code source et le système de suppression des informations d'identification (adresses e-mail, robots Telegram, etc.),
  - Les graphiques proviennent-ils de l'un des sites Web légitimes de l'entreprise ou sont-ils stockés localement ?

Si possible, dans le cas où les graphismes sont tirés de l'un des sites Web de l'entreprise, modifier les graphiques pour afficher un logo "SITE WEB PHISHING" sur la page du fraudeur.

3. Confinement

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

→ Diffuser l'URL de l'attaque en cas de site de phishing,
- Utiliser tous les moyens disponibles pour diffuser l'URL frauduleuse sur chaque navigateur Web,
- Utiliser les options d'Internet Explorer, Chrome, Safari, Firefox, la barre d'outils Netcraft, Phishing-Initiative, etc.,
- Ces actions empêcheront les utilisateurs d'accéder au site malveillant pendant la phase de correction.

Diffuser le contenu frauduleux des e-mails sur des sites Web/partenaires de signalement de SPAM.

→ Communiquer avec les clients :
- Déployer une page d'alerte ou d'avertissement avec des informations sur l'attaque de phishing en cours.

En cas de hameçonnage récurrent (une fois par semaine), ne pas toujours déployer un message d'alerte mais plutôt une page de phishing très informative pour sensibiliser.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

→ Si les pages frauduleuses sont hébergées sur un site Web compromis, essayer de contacter le propriétaire du site Web,
- Expliquer clairement la fraude au propriétaire, afin qu'il prenne les mesures appropriées,
- Supprimez le contenu frauduleux, et surtout améliorer la sécurité sur celui-ci, afin que le fraudeur ne puisse pas revenir en utilisant la même vulnérabilité.

→ Dans tous les cas, contacter également l'hébergeur du site,
- Envoyer un courriel aux adresses de contact de l'hébergeur (en général il y a un abuse@hostingcompany) puis avoir quelqu'un au téléphone, pour accélérer les choses,

→ Contacter la société d'hébergement de messagerie pour fermer les comptes frauduleux. Ne pas oublier de transmettre une copie du courriel malveillant,

→ Contacter l'équipe d'abus du réseau social pour fermer les comptes frauduleux,

→ Bloquer l'échange de courriel avec l'entreprise ou la personne,

Si il n'a pas de réponse ou si aucune mesure n'est prise, ne pas hésiter à rappeler et à envoyer des e-mails régulièrement,

Si le retrait est trop lent, contacter le CERT local du pays qui pourrait aider à éliminer la fraude , en expliquant les problèmes rencontrés.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

5.1. Évaluer la fin de l'incident

- → S'assurer que les pages et/ou l'adresse e-mail frauduleuses sont hors ligne,
- → S'il existe un site Web frauduleux associé à la fraude, continuer à le surveiller,
- → À la fin d'une campagne de SCAM, supprimer la page d'avertissement associée du site Web de l'entreprise.

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.