aDvens

Security for the greater good

Phishing

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.

- → Préparer une communication, prête à être publiée à tout moment, pour avertir les collaborateurs d'une attaque de phishing en cours,
- → Déployer DKIM, DMARC et SPF sur toute la chaîne de messagerie,
- → Mettre en œuvre des mécanismes d'authentification multi-facteurs,
- → Surveiller les domaines typo-squattés et le contenu qui y est publié. Rassembler les informations de contact et d'abus pour se préparer si besoin.

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.

1.2. Interlocuteurs externes

- → Avoir plusieurs moyens pour être joint en temps opportun (24/7 si possible) :
  - Avoir une adresse e-mail facile à retenir pour tous (ex : sécurité@entreprise),
  - Avoir un formulaire sur le site Web de l'entreprise (l'emplacement du formulaire est important, pas plus de 2 clics de la page principale),
  - Avoir un 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 à jour une liste de contacts avec des CERTs à travers le monde, ils pourront en cas d'incident être en mesure d'apporter une 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.

- → Lancer des campagnes périodiques de sensibilisation au phishing,
- → Déployer une solution technique permettant aux collaborateurs de signaler facilement les courriels aux équipes de sécurité,
- → Établir des procédures spécifiques pour l'analyse des pièces jointes et des URL.

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. Étendue des attaques de phishing

- Déterminer le nombre d'utilisateurs ciblés,
- Rechercher les comptes compromis exploités et identifier les activités malveillantes associées.

2.3. Analyse du phishing

Ne pas oublier de suivre les procédures d'analyse établies.

- Déterminer
  - S'il s'agit d'une campagne de collecte d'informations d'identification ou d'une campagne de propagation de logiciels malveillants,
  - S'il s'agit d'une campagne ciblée ou non.
- Inspectez l'objet et le corps du message.
- Utiliser l'environnement sandbox pour analyser les pièces jointes malveillantes et extraire les IOC,
- Analyser les liens, les domaines et les noms d'hôte avec des services de renseignements sur les menaces,
- Vérifier le code source du site Web de phishing,
- Rechercher dans les en-têtes d'e-mails des artefacts intéressants : informations sur le serveur d'origine et l'expéditeur, par exemple.

2.4. 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 stratagème de phishing, pas seulement la première s'il y en a plusieurs. Si nécessaire, faire des captures d'écran des pages.

Pour plus de détails voir l'IRM-07, détection de malware sur Windows, si la campagne de phishing distribue des logiciels malveillants.

3. Confinement

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

- → Bloquer les IOC réseau découverts via l'analyse des pièces jointes / URL sur DNS, pare-feu ou proxies,
- → Bloquer la campagne de phishing en fonction des expéditeurs, des sujets ou d'autres artefacts de messagerie via la passerelle de messagerie,
- → Essayer de supprimer les e-mails de phishing de la boîte de réception,
- → Mettre en place du DNS Sinkhole sur l'URL suspecte (facultatif selon l'architecture DNS),
- → Communiquer avec les collaborateurs,
- → Déployer une page d'alerte/avertissement avec des informations sur l'attaque de phishing en cours.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

- → Modifier et/ou bloquer temporairement les identifiants de connexion des comptes compromis,
- → Si la campagne d'hameçonnage était ciblée, porter plainte,
- → Envisager de contacter un CERT.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Évaluer la fin du phishing

- → S'assurer que les pages et/ou l'adresse e-mail frauduleuses ne sont plus actives,
- → Continuer à surveiller l'URL frauduleuse. Parfois, un site Web de phishing peut réapparaître quelques heures plus tard. Dans le cas où une redirection est utilisée et non supprimée, la surveiller de très près.

A la fin de la campagne de phishing, s'assurer que l'ensemble des éléments associés sont bien supprimés.

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.