REMISE EN ETAT DE FONCTIONNEMENT DU SI

Annulation des actions menées en phase de “confinement” & “remédiation”

L’objectif est de rétablir le système dans l’état ou il se trouvait avant l’incident.
Il est donc nécessaire de supprimer les traces des actions de confinement et de remédiation menées par l’équipe de réponse à incident (par exemple les règles de filtrage, etc..).

PREPARATION

Veille technologique

- Déploiement / Validation de nouveaux outils
- Veille de nouvelles techniques d’exploitation (MITRE ATT&CK)

Entrainement

- Déploiement de plateforme d’Investigation
- Test et vérification des procédures déjà établies

Documentation / Procédures

Enrichir la documentation et les procédures à partir des actions menées ci-dessus

IDENTIFICATION

Détection d’un événement

- Un usager reçoit un mail d’hameçonnage
- Une sonde réseau détecte une utilisation de la bande passante anormalement élevée
- Une sonde réseau détecte une attaque

Identification de l’impact sur le SI

Il y a un “Incident de sécurité” lorsqu’il y a un impact sur une ressource de notre système d’information :

Confidentialité / Disponibilité / Intégrité

Identification des IOCs

- Analyse des systèmes de détection réseau
- Analyse de la mémoire vive
- Analyse des périphériques de stockage

Définir le périmètre & IOC

Il est indispensable de définir le périmètre de l’incident avant de mener des actions de remédiation et/ou de confinement !!

Le périmètre peut être identifié en utilisant les IOCs obtenus lors des premières investigations.

CONFINEMENT

Définition des actions à mener

Le confinement est une action délicate qui permettra de limiter, voir stopper la progression de l’attaquant sur le système d’information.

Il est indispensable d’identifier chacunes des actions qui devront être menées avant de les appliquer

Application des actions

Elles peuvent être de natures différentes :

- Désactivation de l’accès réseau aux ressources impactées
- Application de règles de filtrage au sein d’un pare-feu et/ou d’un IPS
- Désactivation des services et/ou des logiciels ayant servis de points d’entrée ou ayant permis à l’attaquant d’étendre son contrôle.

Attention

L’attaquant peut percevoir votre intention et entreprendre en retour des actions irréversibles sur les données de votre systèmes d’informations.

REMEDIATION

Définition des actions à mener

La phase de remédiation consiste à effectuer des actions pour supprimer toutes traces liées à l’incident.

Il est indispensable d’identifier chacunes des actions qui devront être menées avant de les appliquer

Application des actions

Elles peuvent être de natures différentes :

- Suppression des binaires recensés durant la phase d’identification.
- Reinitialisation des comptes utilisateurs et services utilisés par l’attaquant.
- Mise à jour des systèmes d’exploitation du SI
- ..

Attention

Il est important de valider chacunes des actions qui devront être menées avec la direction. Celles-ci peuvent en effet avoir un impact sur la disponibilité du SI.

RETOUR D’EXPERIENCE

Historisation des actions

L’objectif de cette étape est de recenser toutes les actions menées de la phase d’identification jusqu’à maintenant. Elles incluent les actions de l’attaquant comme celles de l’équipe de réponse à incident.

- Quelles actions ont été réalisées par l’attaquant ?
- Quelles actions avons-nous menées ?

Définition d’axes d’amélioration

A partir du recensement effectué à l’étape précédente, il est temps de dresser un premier bilan. Quels sont les axes d’amélioration à apporter à nos procédures actuelles ?

- Que pouvons-nous améliorer ?
- Qu’aurions-nous pu faire de plus ?
- Que ferons-nous différemment la prochaine fois ?

RED TEAM

Il peut être util pour une “RED TEAM” de pouvoir bénéficier de votre retour d’expérience sur le schéma d’attaque rencontré lors de votre réponse à incident.
Le partage dans ce type de situation est indispensable.