Incident de Sécurité : Fiche Réflexes

Introduction

Cette méthodologie séquence les actions communes à opérer quel que soit la nature de l’incident de cybersécurité rencontré.

L’essentiel est de garder son calme, circonscrire la compromission et de ne surtout pas éteindre les machines infectées, cela ferait perdre les informations nécessaires aux investigations.

Etape 1 Identifier les acteurs nécessaires – pour l’efficacité dans la gestion de crise **limiter au strict minimum** les acteurs à contacter

Une fois les acteurs identifiés envoyer les invitations à la « cellule de crise » et passer le relais.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nom | Prénom | Rôle | Téléphone | Mail | | Commentaire |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |
|  |  |  |  | |  |  |

Etape 2 Structurer la comitologie et identifier les porteurs d’actions

* Initialisation de la crise
  + Objectifs :
    - Définir les périmètres
    - Confirmer les acteurs
    - Définir la fréquence des mises à jour
* Cellule de crise technique *(maximum 6 pers)*
  + Objectifs :
    - Circonscrire l’incident
    - Créer les comptes pour le CERT / l’analyse des logs
* Cellule de crise commercial et marketing *(maximum 6 pers)*
  + Objectifs :
    - Communiquer aux utilisateurs internes du services
    - Communiquer aux clients impactés
* Cellule de crise managérial *(maximum 6 pers)*
  + Objectifs :
    - Donner les arbitrages nécessaires

Etape 3 Confinement

Couper tous les flux de la ou des machines compromises.

Forcer la rotation de tous les mots de passes compromis.

Répéter l’opération sur toutes les machines potentiellement atteintes.

Etape 4 Contacter le CERT

Appeler le numéro indiqué

Leur créer les accès nécessaires aux investigations :

• Infrastructure

• Réseaux/firewall/EDR/anti-virus

• Administration des systèmes

• Annuaires

• Accès à privilège

• Cloud / SaaS 365

• Sécurité

Etape 5 Main courante

|  |  |  |
| --- | --- | --- |
| Date/Heure (Locale) | Observation/action | Acteur |
| jj/mm/aaaaa hh:mm | Réunion de qualification |  |
| jj/mm/aaaaa hh:mm | Mise en place de la gestion de crise |  |
| jj/mm/aaaaa hh:mm | Réunion de synchronisation (crise) |  |
| jj/mm/aaaaa hh:mm | Création compte EDR |  |
| jj/mm/aaaaa hh:mm | Création compte AD/ANTIVIRUS |  |
| jj/mm/aaaaa hh:mm | Test des accès EDR et ANTIVIRUS |  |
| jj/mm/aaaaa hh:mm | Réunion de synchronisation (crise) |  |
| jj/mm/aaaaa hh:mm |  |  |
| jj/mm/aaaaa hh:mm |  |  |

Etape 6 Suivi des actions :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Création** | **Type** | **Action** | **Responsable** | **Priorité** | **Status** | **Dépendance** | **Détail** |
| **dd/mm/aaaa hh:mm** | **Endiguement** | **Isolement de toutes les machines** |  | **P0** |  |  |  |
| **dd/mm/aaaa hh:mm** | **Endiguement** | **Rotation des mots de passe** |  | **P0** |  |  |  |
| **dd/mm/aaaa hh:mm** | **Entrants I&R** | **Accès EDR** |  | **P0** |  |  |  |
| **dd/mm/aaaa hh:mm** | **Entrants I&R** | **Accès ANTIVIRUS** |  | **P0** |  |  |  |
| dd/mm/aaaa hh:mm | Communication | Communication interne |  | P1 |  |  | Uniquement si impact des équipes internes |
| dd/mm/aaaa hh:mm | Communication | Communication clients |  | P1 |  |  | Ne pas s'engager sur la remise en service mais plutôt sur la fréquence d'un état de situation. |
| **dd/mm/aaaa hh:mm** | **Administratif** | **Contacter l'assurance CYBER** |  | **P2** | **En cours** |  |  |
| **dd/mm/aaaa hh:mm** | **Administratif** | **Prédéclaration CNIL** |  | **P2** | **En attente** |  |  |
| **dd/mm/aaaa hh:mm** | **Administratif** | **Dépôt de plainte** |  | **P2** | **En attente** |  |  |
| dd/mm/aaaa hh :mm |  |  |  |  |  |  |  |
| dd/mm/aaaa hh :mm |  |  |  |  |  |  |  |
| dd/mm/aaaa hh :mm |  |  |  |  |  |  |  |