Shape

Description automatically generatedText

Description automatically generated with low confidence

|  |
| --- |
| Sylvain Depasse  1-9-2023 |

|  |
| --- |
| Annex IRP2 |
| IRP2 Identifiants Compromis |
| Incident Respons Plan 2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **CYBERSECURITE** | | |
| **POLITIQUE** | **IRP2 Identifiants Compromis** | | | |
| **Policy ID:** | **Add ID Number** | **Date de création: 8/24/2022** | | |
| **Approved by:** |  | **Reviewed**  **(No changes made)** | **☐** | **Date** |
| **Approved by:** |  | **Revised**  **(Changes made)** | **☐** | **Date** |
| **Area:** | **Choose Area** | **Repealed**  **(No longer active)** | **☐** | **Date** |
| **Department:** | **Choose Department** | **Prior Policy: N/A** | | |
| **Applies to:** | **All Areas** |  | | |
|  | | | | |
| **Additional Approvals**  Additional reviews and approvals by internal and external stakeholders. | | | | |
| **Approver Title** | | **Area / State / Agency** | | |
|  | |  | | |
|  | |  | | |
|  | | | | |
| **Data Classification:** **Confidential** | | **Electronic Approvals are maintained in the Policy Repository** | | |
|  | | | | |
| **Additional Information:** | | | | |
|  | | | | |
|  | | | | |

Contents

[1 Introduction 3](#_Toc125977946)

[2 Définitions : 3](#_Toc125977947)

[3 Identification : 3](#_Toc125977948)

[4 Evaluation : 3](#_Toc125977949)

[5 Réponse : 3](#_Toc125977950)

[6 Recovery : 3](#_Toc125977951)

[7 Revue après action : 3](#_Toc125977952)

[8 Références aux Régulation et Standards 3](#_Toc125977953)

[9 Références aux autres documents internes 3](#_Toc125977954)

[10 Autres références externes 3](#_Toc125977955)

# Introduction

Ce document fait suite en complément au Respons Incident Plan et vous y trouverez une stratégie afin de résoudre un souci de confidentialité d’identifiant suite à une fuite quelconque (phishing, BrutForce,..)

Afin de faciliter votre avancement, munissez-vous de DIR2.

La procédure suivante est organisée en étapes logiques plus à des fins d'organisation qu'une chronologie stricte du moment où les choses doivent se produire. De nombreuses étapes du processus suivant peuvent se produire et se produiront simultanément, et ce n'est pas grave. S'il est logique d'effectuer une étape avant les autres, faites-le tant que toutes les actions pertinentes se produisent. Un exemple de ceci est que le confinement initial se produit généralement avant que l'identification ne soit terminée.

Retenez bien qu’il est important de documenter vos actions ainsi que le fruit de vos actions.

!! Les règles d’accomplissement renseignées dans le Plan De réponse aux incidents dont il est l’annexe devront être suivies !!

# Définitions :

Ioc : indicateurs de compromissions (Hachage de fichiers, IP, domaine, ID,…

MDP : Mots De Passe

Malware : Logiciel malveillant

# Identification :

Afin de déterminer la méthode initiale de compromission du compte vous pouvez :

* Interviewer l’utilisateur impacté pour recueillir des détails sur les points de compromission potentiels (cette étape peut vous éviter de perdre du temps dans la recherche)  
  Voici quelques exemples utiles :
  + Avez-vous reçu un mail suspect ?
  + Avez-vous entré vos identifiants (de messagerie par exemple) après avoir cliqué sur un lien, ou un site Web que semblait ne pas les accepter ?
  + Avez-vous téléchargé un nouveau logiciel ?
  + Avez-vous reçu des documents par mail auxquels vous ne vous attendiez pas spécialement ?
  + Avez-vous remarqué des actions anormales sur le plan de travail ?

Si cette étape ne suffit pas à déterminer la méthode initiale, il vous faudra procéder à des recherches.

* Rechercher des mails de phishing.
* Effectuer une recherche dans l’historique web afin de vérifier si l’utilisateur n’a pas visité de sites malveillants.
* Recherche de malware sur la machine (sniff , mimikatz, keylocker, …)
  + !!En cas de ransomware, utilisé l’annexe IR4 !!

Détermination de la méthode initiale terminée (vous savez comment) :

* Utilisez les IOC afin de de rechercher d’éventuelles autres victimes
* Examinez les journaux dans les systèmes de connexions de compte à la recherche d’anomalies.
  + Activité de connexions inhabituel (emplacement, méthode,..).

Notez tous les systèmes de connexions auxquels l’attaquant a eu accès.

# Evaluation :

Utilisez les éléments récoltés afin d’évaluer le degré de gravité.  
   
Effectivement, à cette étape, vous devriez être à même de savoir à quoi l’attaquant a réellement eu accès, et donc s’il y a des données sensibles stockées dans les environnements qui lui sont ou lui ont été accessibles.  
Si les logs confirment une connexion, nous supposerons que les données ont été consultées par l’attaquant.

# Réponse :

* Réinitialisé tous les mots de passe associées à toutes les victimes identifiées.
  + Commencez par les MDP de compte compromis connus, mais tous les associés à l’utilisateurs doivent voir leur MDP réinitialisés ou désactivés.
* Activez l’authentification multi facteur partout où cela est possible pour l’utilisateur concerné.
* Désactivez la capacité du compte utilisateur à se connecter à distance.
* Révoquez les jetons d’authentifications pour tous les comptes des victimes identifiées.
* Dans le cas où une organisation externe est identifiée au cours de l’enquête :
  + Informez-la de toute compromission ou suspicion de compromission.
  + Empêchez ses domaines associés d’envoyer des mails à votre organisation.
* Si un malware est détecté lors de l’enquête :
  + Conservez un échantillon de celui-ci (fichiers suspectés d’être infectés)
  + Analysez le malware   
    Exemple : soumettez le hachage aux sources com (VirusTotal, Hybridanalysis,..) afin d’en récupérer les caractéristiques
* Isolez les systèmes infectés, ne les éteignez pas sauf ordre de (voir Mr Vander Elst) conservez une copie de ces systèmes et les éléments recueillis pour une enquête plus approfondie (analyse malware, logs, IP, copie des SSD, disque physique ..)
* Bloquez tous les IoC associés dans les systèmes de messagerie, firewall, anti-virus,..

# Recovery :

* Assurez-vous d’avoir conservez toutes les données utiles.
* Remplacez ou reconstruisez les systèmes en conséquence.
  + Restaurez les systèmes affectés à partir d’une sauvegarde propre, prise avant l’infection si ces sauvegardes sont disponibles.
  + Pour les systèmes qui ne peuvent être restaurés à partir d’une sauvegarde, reconstruisez les machines à partir d’une bonne image, ou à partir d’un système nu.
  + Corrigez les vulnérabilités et lacunes recensée au cours de l’enquête.
  + Réinitialisez les MDP des tous les comptes concernés ou créez des comptes de remplacement et laissez les comptes concernés désactivé » de façon permanente.

Après le redémarrage, assurez un monitoring afin de surveiller l’activité liée à ce même incident.

# Revue après action :

Pour cette étape référez-vous au RAA1

# Références aux Régulation et Standards

Les références aux standards internationaux et régulation relatives au secteur de l’entreprise sont repris dans le tableau ci-dessous.

|  |  |  |
| --- | --- | --- |
| **ISO 27001:2013** | **NIST SP 800-53** | **HIPAA** |
| A.8.1.3 Acceptable Use of Assets | AC-20, PL‑4, PS-6 | Workstation Use §164.310(b) |

# Références aux autres documents internes

Les références à d’autres politiques, standards, procédures ou documents internes sont listées dans le tableau ci-dessous.

|  |  |
| --- | --- |
| **Document Name** | **Document ID** |
| Diagrame Incident Respons 2 | DIR2 |
| Incident Respons Plan | IRP |

# Autres références externes

Les références utilisées ou citées durant la rédaction de ce document sont listées dans le tableau ci-dessous.

|  |  |  |  |
| --- | --- | --- | --- |
| **Référence** | **Titre** | **ID de Référence** | **Année** |
|  |  |  |  |