Shape

Description automatically generatedText

Description automatically generated with low confidence

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

|  |
| --- |
| Annex IRP3 |
| IRP3 WebApp |
| Incident Respons Plan 3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **CYBERSECURITE** | | |
| **POLITIQUE** | **IRP3 WebApp** | | | |
| **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| **Area:** | **Choose Area** | **Repealed**  **(No longer active)** | **☐** | **Date** |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](#_Toc125979181)

[2 Définitions : 3](#_Toc125979182)

[3 Identification : 3](#_Toc125979183)

[4 Evaluation : 3](#_Toc125979184)

[5 Response : 3](#_Toc125979185)

[6 Recovery : 3](#_Toc125979186)

[7 Revue après action : 3](#_Toc125979187)

[8 Références aux Régulation et Standards 3](#_Toc125979188)

[9 Références aux autres documents internes 3](#_Toc125979189)

[10 Autres références externes 3](#_Toc125979190)

# Introduction :

Ce document fait suite en complément au Respons Incident Plan et vous y trouverez une stratégie afin de résoudre un souci de WebApp.

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.

Afin de faciliter votre avancement, munissez-vous de DIR3.

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

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

# Définitions :

# Identification :

* Si l’application WEB est hébergée sur un autre service d’hébergement, contacter le pour lui signaler le problème.
  + Renseignez-vous sur les problèmes de sécurité récents dans leur environnement
  + Demandez à recevoir les données qu’ils possèdent en rapport aux dernière attaques similaires
* Utilisez les preuves (comportement anormal dans l’app, notif de compromission, signalement client,) pour déterminer les prochaines étapes en fonction de la méthode de compromission (exploit, brut force, config,..)

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’ 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 e 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 initial 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 auxquels l’attaquant a eu accès
* Si la compromission du compte a été exclue, procédez à une enquête sur les vulnérabilités potentielles des WebApp qui pourraient avoir été exploitées.
  + Effectuez une analyse de sécurité
  + Examinez les notifications des fournisseurs concernant les problèmes de sécurité.
  + Examinez les renseignements sur les menaces provenant de la communauté et liés aux composants de votre WebApp

# Evaluation :

* En cas de détermination d’une compromission du compte de gestion ou admin :
  + Réinitialisez tous les MDP associés à la gestion et à l’administration de l’App, en commençant par le MDP du compte compromis connu
  + Activez l’authentification multifacteur partout où il est possible de le faire
  + Désactivez ou réinitialisez les méthodes d’authentification alternatives
  + Révoquer les jetons d’authentifications pour ces même comptes.
* 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
* Bloquez tous les IoC associés dans les systèmes de messagerie, firewall, anti-virus,..
* Conservez une copie de tout code de WebApp existant susceptible d’être compromis et/ou modifié de manière malveillante.

# Response :

* Comparez le code d’App actuel à une copie connue pour déterminer si des ajouts malveillants sont ou doivent être supprimés.
* 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
    - !!En cas de ransomware, utilisé l’annexe IR4 !!

Conservez toutes les données relatives à l’incident

# Recovery :

Afin de procéder à une récupération des systèmes :

* Remplacez le code D’app potentiellement compromis par une copie en bon état
* Examinez le code afin de vous assurer que toutes les anomalies ont bien été supprimées (examen de sécurité)
* Restaurer la fonctionnalité de la WebApp

Pour les services qui ne peuvent pas 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 de 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** |
| Non-discrimination and Anti-harassment Policy |  |

# 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** |
|  |  |  |  |