Shape

Description automatically generatedText

Description automatically generated with low confidence

|  |
| --- |
| Sylvain Depasse  1-30-2023 |

|  |
| --- |
| Annex IRP1 |
| IRP1 Phishing |
| Incident Respons Plan 1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **CYBERSECURITE** | | |
| **POLITIQUE** | **IRP1 Phishing** | | | |
| **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| **Area:** | **Choose Area** | **Repealed**  **(No longer active)** | **☐** | **Date** |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](#_Toc125980966)

[2 Définitions 3](#_Toc125980967)

[3 Identification 3](#_Toc125980968)

[4 Evaluation 3](#_Toc125980969)

[5 Réponse 3](#_Toc125980970)

[6 Recovery 3](#_Toc125980971)

[7 Revue après action 3](#_Toc125980972)

[8 Références aux Régulation et Standards 3](#_Toc125980973)

[9 Références aux autres documents internes 4](#_Toc125980974)

[10 Autres références externes 4](#_Toc125980975)

# Introduction

Ce document fait suite en complément au Respons Incident Plan et vous y trouverez une stratégie de réponse face à une attaque par phishing.

Afin de faciliter votre avancement, munissez-vous de DIR1.

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

# Identification

Nous savons qu’il est question ici d’une attaque par phishing. Cependant il nous faut encore définir le type de phishing

Afin de déterminer le type de phishing dont nous sommes victimes, interviewer l’utilisateur impacté.

Prenez des notes sur le ou les problèmes à l'aide de l'application de mémo vocal sur votre smartphone ou avec un stylo et du papier. S'il s'agit d'un rapport d'utilisateur, posez des questions détaillées, notamment :

1. Qu'avez-vous remarqué ?
2. Pourquoi avez-vous pensé que c'était un problème?
3. Que faisiez-vous au moment où vous l'avez détecté ?
4. Quand s'est-il produit pour la première fois et combien de fois depuis ?
5. Quels réseaux sont concernés ? (bureau/domicile/magasin, filaire/sans fil, avec/sans VPN, etc. )
6. Quels sont les systèmes concernés ? (système d'exploitation, nom d'hôte, etc. )
7. Quelles sont les données concernées ? (chemins, types de fichiers, partages de fichiers, bases de données, logiciels, etc. )
8. Quels utilisateurs et comptes sont concernés ? (Active Directory, SaaS, SSO, comptes de services, etc. )
9. À quelles données les utilisateurs concernés accèdent-ils généralement ?
10. Qui d'autre avez-vous contacté à propos de cet incident, et que leur avez-vous dit ?

 Obtenez les coordonnées détaillées de l'utilisateur (domicile, bureau, mobile), le cas échéant.

 Enregistrez toutes les informations dans le ticket, y compris les notes manuscrites et vocales.

Faites une analyse malware sur la machine !

 !!En cas de ransomware, utilisé l’annexe IR4 !!

* 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

Une attaque par phishing résultera sur un type d’attaque. Tournez-vous vers les documents correspondants.

En cas de MDP Compromis, munissez vous de IR2 et DIR2

En cas de WebApp Compromise, munissez vous de IR3 et DIR3

En cas de présence de ransomware, munissez vous de IR4 et DIR4

Pour tout autre Malware, munissez vous de IR5 er DIR5

# Recovery

Suivez les procédure de reprise des activités reprise sur les plan en rapport à l’incident

# Revue après action

Pour cette étape référez-vous au RAA

# 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** |
|  |  |  |  |