Shape

Description automatically generatedText

Description automatically generated with low confidence

|  |
| --- |
| Sylvain Depasse  2-3-2023 |

|  |
| --- |
| Annex IRP4 |
| IRP4 Ransomware |
| Incident Respons Plan 4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **CYBERSECURITE** | | |
| **POLITIQUE** | **IRP4 Ransomware** | | | |
| **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| **Area:** | **Choose Area** | **Repealed**  **(No longer active)** | **☐** | **Date** |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](#_Toc126318799)

[2 Définitions 3](#_Toc126318800)

[2.1 3](#_Toc126318801)

[3 Identification : 3](#_Toc126318802)

[3.1 Détection : 3](#_Toc126318803)

[3.2 Analyse : 3](#_Toc126318804)

[4 Evaluation : 3](#_Toc126318805)

[5 Réponse : 3](#_Toc126318806)

[5.1 Confinement : 3](#_Toc126318807)

[5.2 Eradication : 3](#_Toc126318808)

[6 Recovery : 3](#_Toc126318809)

[7 Revue Après Action : 3](#_Toc126318810)

[8 Références aux Régulation et Standards 3](#_Toc126318811)

[9 Références aux autres documents internes 3](#_Toc126318812)

[10 Autres références externes 3](#_Toc126318813)

# Introduction :

**!Attention !**

!Payer une rançon ne garantit pas que vous serez secouru, et cela n'implique pas que vous serez secouru immédiatement.!

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

Afin de faciliter votre avancement, munissez-vous de DIR4.

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 :

EDR =>

IDS =>

Sysmon =>

FIM =>

ACR => Analyse des Causes Profondes

CIO => Chief Informatique Officer

# 

# Identification :

Pour l’étape d’identification, nous tenterons de déterminer la variante du logiciel présent afin de récolter des informations à son sujet et donc faciliter la réponse de l’équipe CERT.

L'identification de tous les systèmes infectés, ainsi que ceux en danger immédiat d'infection, est le problème le plus urgent au début de l'attaque pour identifier les risques éventuels et les actifs ou utilisateurs concernés

* + Mettez les comptes compromis sous surveillance.
  + Liste des hôtes communiquant avec une IP externe, une URL externe, un domaine externe.
  + Répertoriez les utilisateurs qui ont ouvert un e-mail suspect et collectez tous les e-mails.
  + Répertoriez tous les destinataires des e-mails.
  + Assurez-vous que le message électronique est un phishingmail.
  + Extraire les observables des messages électroniques.

Pour comprendre comment le rançongiciel s'est introduit dans l'environnement, procédez à une étude de cause initiale. Il est important de déterminer si la vulnérabilité provient d'un e-mail ou d'un navigateur Web.

Le CERT doit garder à l'esprit que même si le blocage du site malveillant identifié est la première étape, il se peut qu'il ne s'agisse pas d'un contrôle compensatoire adéquat puisque les employés mobiles ne seront pas bloqués par les règles de pare-feu de l'organisation tant qu'ils ne se trouvent pas sur le réseau local de l'organisation (LAN ). Il faudra donc communiquer avec le personnel nécessaire.

La recherche de modèles de noms de fichiers aléatoires ou d'extensions de rançon connues est un autre moyen de détecter le ransomware en cours d'exécution.

Des clés de registre étranges, des fichiers malveillants, des données cryptées, des quantités inhabituelles de flux de trafic interne, des pannes système inexpliquées, des installations de logiciels illégales et inexpliquées, des applications ou des fichiers non-inscrits sur la liste blanche sont tous des exemples d'opérations manuelles.

Les journaux EDR, les journaux de trafic réseau entrant/sortant, les journaux d'événements Windows, les journaux SIEM, les journaux système et les sources de renseignements sur les menaces doivent être surveillés de manière intensive.

* + Mettez les comptes compromis sous surveillance.
  + Liste des hôtes communiquants avec une IP externe, une URL externe, un domaine externe.
  + Répertoriez les utilisateurs qui ont ouvert un e-mail et collectez tous les e-mails. Répertorier tous les destinataires des e-mails. Assurez-vous que le message électronique est un phishingmail. Extraire les observables des messages électroniques.

# 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 :

Pour ce plan, j’ai divisé le processus de réponse en 2 étapes distinctes comme suit :

Confinement/Eradication

# Confinement :

* Si le ransomware est déjà exécuté avec son cryptage et son message, vous pouvez prendre des mesures pour le contenir localement afin que les fichiers réseau ne soient pas affectés.
* Rechercher l'exécution et de tuer le processus est généralement le meilleur moyen de confinement.
* Une fois qu'un système a été identifié comme potentiellement porteur d'un rançongiciel, l'ordinateur potentiellement infecté doit être immédiatement retiré de vos réseaux (y compris le Wi-Fi) et soit arrêté, soit idéalement mis en veille prolongée (pour faciliter l'analyse médico-légale et l'analyse d'échantillons) afin de minimiser le risque que le rançongiciel poursuive le processus de cryptage.
* Si le point ci-dessus ne s'applique à aucune organisation, la mise hors ligne des partages de fichiers contribuera à minimiser les risques et l'impact sur l'entreprise. Les serveurs de fichiers n'ont pas besoin d'être arrêtés, mais tous les accès aux partages de fichiers doivent être interrompus (supprimer le partage, restreindre par réseau, etc.).

# Eradication :

Cette phase consiste à supprimer le ransomware des systèmes infectés. Après avoir confiné la/les machine(s) infectée(s), nous devons l'éradiquer du réseau.

* La machine infectée identifiée avec le rançongiciel peut être reconstruite à partir d'une source fiable.
* Il est préférable de remplacer ou de réimager la machine plutôt que de la nettoyer. Si nous choisissons de nettoyer plutôt que de remplacer, continuez à surveiller les signatures et autres IOC pour empêcher l'attaque de réapparaître.
* Nécessité de prendre des mesures suite à l’analyse de cause initiale. Si c'est par e-mail, vous devez supprimer tous les e-mails qui s'y rapportent. S'il s'agit d'un exploit de navigateur Web, ces sites doivent être bloqués et surveillés. L'organisation doit alors déterminer si des composants de navigateur vulnérables doivent être mis à jour ou supprimés.
* Par mesure de précaution, les mots de passe de tous les utilisateurs concernés doivent être modifiés. Pour éviter d'alerter les attaquants, cette action doit être menée avec prudence et intelligence. Il est probable qu'un attaquant dispose de plusieurs ensembles d'informations d'identification et peut tenter de les utiliser et faire pivoter l'attaque si son accès initial est soudainement révoqué.

# Recovery :

Cette étape reprendra des points du paragraphe 5 ‘reponse’, car effectivement lors de l’étape 5 il se peut que vous ailliez besoin de réinstaller. Ce plan ne peut couvrir tous les scenarios spécifiques simultanément.   
Cependant ne passez pas celui-ci, il y aura des étapes utiles et indispensables.

Il s'agit du processus de restauration et de retour des systèmes et appareils concernés dans votre environnement professionnel. Pendant ce temps, il est important que vos systèmes et vos opérations commerciales soient à nouveau opérationnels sans craindre une autre violation.

* Restaurez à partir d'une sauvegarde propre.
* En fonction des résultats de l'analyse des causes profondes, si l'attaque a été rendue possible par des systèmes vulnérables, ceux-ci doivent être corrigés pour éviter qu'ils ne soient réexploités à l'avenir.
* Il est essentiel de vérifier l'état des sauvegardes lorsqu'une restauration est nécessaire. L'utilisation de sauvegardes pour restaurer les systèmes n'est pas une solution réaliste si les attaquants sont sur les réseaux depuis des mois et que les données de sauvegarde sont également cryptées.
* La redondance est une bonne pratique pour les sauvegardes, tout comme la vérification, la séparation ou la mise hors ligne des sauvegardes pour réduire le risque de manipulation.
* L'inversion du chiffrement peut être effectuée dans les cas où une sauvegarde complète est impossible. Les organisations peuvent chercher à trouver des moyens de casser le chiffrement sans payer la rançon, ou peut-être localiser des clés de déchiffrement sur des systèmes infectés.

# 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** |
|  |  |  |  |