cyna
secure your future

Fuite de données

Méthodologie de réponse à incident

IRM-04 08/09/2023

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

- La fiche IRM s'adresse aux personnes ou fonctions suivantes :
  - Les RSSI et leurs adjoints
  - Les DSI et leurs adjoints
  - Les administrateurs

Rester calme et contacter immédiatement l'équipe de réponse à incident Cyna.
Nos canaux de discussion :

- **Cybersecurity@cyna-it.fr**
- **+33 9 70 70 41 81 (Heure ouvrés)**

En cas d'urgence, veuillez insérer la balise [URGENT] dans l'objet du courriel. Veuillez noter que notre CERT est disponible 24 heures sur 24 et 7 jours sur 7, mais que l'assistance téléphonique n'est pas disponible en dehors des heures de bureau.

Politique de sécurité

Objectif :

Garantir que la valeur des informations de l'entreprise est clairement définie et intégrée dans le règlement intérieur, la charte informatique, ainsi que lors des sessions de sensibilisation et de formation.
Cette démarche implique l'identification de l'ensemble des actifs de valeur au sein de l'organisation.

En conclusion, il est fortement recommandé de vérifier que le processus d'escalade des incidents de sécurité est bien établi et que les responsabilités des parties prenantes sont clairement attribuées.

Identification

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

La fuite de données peut se produire de n'importe où. Cela peut être un employé qui contourne volontairement ou non les problèmes de sécurité, ou un ordinateur compromis.

1. Détection initiale : Expliquez comment l'incident de fuite de données a été initialement détecté. Cela pourrait inclure des alertes de sécurité, des rapports d'employés ou d'autres sources.

2. Nature de l'incident : Décrivez brièvement la nature de l'incident de fuite de données, par exemple, s'agit-il d'une perte accidentelle, d'une cyberattaque, d'une violation de la vie privée, etc.

3. Classification de l'incident : Classez l'incident en fonction de sa gravité (par exemple, faible, modérée, élevée) pour évaluer son impact potentiel sur l'organisation.

Processus d'endiguement

1. Isolation immédiate : Détaillez les mesures prises pour isoler l'incident et éviter qu'il ne s'aggrave. Cela pourrait inclure la mise hors ligne de systèmes compromis ou la fermeture de vulnérabilités.

2. Évaluation de l'impact : Expliquez comment l'équipe de réponse à l'incident évalue l'impact de la fuite de données sur l'organisation, y compris les données exposées, les systèmes affectés et les parties prenantes concernées.

3. Identification des sources : Précisez les efforts déployés pour identifier la source de la fuite de données, qu'il s'agisse d'une erreur humaine, d'une activité malveillante, etc.

4. Actions correctives immédiates : Décrivez les actions immédiates entreprises pour limiter davantage la fuite de données et protéger les actifs de l'entreprise.

5. Documentation de l'incident : Expliquez comment les détails de l'incident sont documentés, y compris les journaux d'incident, les preuves numériques et les rapports.

6. Signalement aux autorités compétentes : Si nécessaire, indiquez si l'incident de fuite de données doit être signalé aux autorités compétentes en matière de protection des données ou aux organismes de réglementation.

7. Communication aux parties prenantes : Précisez comment les parties prenantes internes et externes sont informées de l'incident, y compris les employés, les clients, les partenaires commerciaux, etc.

8. Rétablissement : Expliquez comment l'organisation travaille à la remise en état des systèmes affectés, à la restauration des données perdues et à la réduction de la vulnérabilité aux futures fuites de données.