PRÉVENIR UNE FUITE DE DONNES

QU'EST-CE QU'UNE FUITE DE DONNEES ?

Une fuite de données est la transmission non autorisée de données d'une organisation vers un destinataire externe de manière intentionnelle ou fortuite. Les fuites de données se produisent généralement via l'intrusion sur des sites web et l'envoi de courrier électronique, mais peuvent également se produire par la perte ou le vol de périphériques tels que les clés USB ou les ordinateurs portables.

CAUSES POSSIBLES

ACCIDENTELLES :

- Erreur de paramétrage dans la gestion des accès réseau ou des habilitations
- Envoi de données à une personne non autorisée, en copie d'un email par exemple
- Non-respect des bonnes pratiques en matière de destruction de supports papiers ou numériques
- Vol d'un ordinateur

MALVEILLANTES :

- Copie de données par une personne interne à la structure
- Compromission du système d'information pour exfiltrer des données
- Attaque par ingénierie sociale afin de récupérer des données personnelles ou confidentielles
- Intrusion sur un site web

COMMENT RÉAGIR EN CAS DE FUITE ?

- Identifier les sources et le périmètre de la fuite :
  - Conduire une investigation afin d'identifier la source de la fuite (compromission du système d'information, malveillance interne…)
  - Identifier les données qui sont ou peuvent être concernées par la fuite en analysant les journaux d'accès aux données (fiche réflexe « Réagir à une intrusion web » pour les actions post-incident)
  - En l'absence d'une expertise en interne, faire appel à un prestataire pour une analyse post-incident
- Notifier la direction générale en vue d'évaluer les différents impacts sur les personnes et les conséquences juridiques et financières (prévoir le déclenchement d'une cellule de crise selon la gravité de l'incident).
- Se soumettre aux contraintes légales (RGPD – voir la fiche réflexe « Réagir à un acte de cyber-malveillance »)

MESURES DE PRÉVENTION

- Opérationnelles :
  - Réduire les droits d'accès selon le principe de moindre privilège par une solution de gestion des habilitations (Identity Access Management)
  - Déployer un système de gestion de correctifs de sécurité (patch management)
  - Mettre en place des politiques de mots de passe forts
  - Mettre en place l'authentification multi-facteurs
  - Effectuer régulièrement des scans de vulnérabilités et des tests d'intrusion
  - Implémenter des politiques de protection contre les logiciels malveillants et les menaces internes
  - Mettre en place une veille/surveillance afin de détecter d'éventuelles fuites d'informations (interne ou externalisée)
  - Chiffrer le contenu des ordinateurs portables afin de limiter l'impact d'un vol potentiel
- Organisationnelles :
  - Classifier les données pour prendre en compte le niveau de protection requis compte tenu de leur sensibilité
  - Implémenter des politiques de sécurité pour tous les supports de données
  - Evaluer et sécuriser l'exposition sur internet (Fiche réflexe « Sécuriser son exposition sur internet »)
  - Diffuser les contacts à solliciter en cas d'incident et définir un plan d'action en cas de fuite de données couvrant l'évaluation de la fuite (origine, données concernées, criticité…) et une réponse appropriée
- Sensibilisation :
  - Promouvoir l'utilisation du chiffrement des données sensibles lors de leur stockage et de leur transmission
  - Mettre à disposition des utilisateurs des moyens techniques pour chiffrer les données (coffre-fort numérique, etc.)
  - Encourager et faciliter le signalement d'activités suspectes auprès du responsable de sécurité

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

PREVENIR UNE FUITE DE DONNEES

RISQUES

- ➔ **ATTEINTE A LA VIE PRIVÉE DES PATIENTS**
- ➔ **USURPATION D'IDENTITÉ**
- ➔ **DOMMAGES FINANCIERS**
- ➔ **ATTEINTE À L'IMAGE DE LA STRUCTURE DE SANTÉ**

RESSOURCES

Fiche réflexe « Réagir à un acte de cyber-malveillance » : https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiches_reflexes-reagir-cybermalveillancev1.0.pdf

Fiche réflexe « Sécuriser son exposition sur internet » : https://www.cyberveille-sante.gouv.fr/fiches-reflexes/1117-securiser-son-exposition-sur-internet-2018-12-13

Fiche réflexe « Réagir à une intrusion web » : https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/fiches-reflexes/Fiches_reflexes-intrusion_web-v1.3.pdf

Site Have I Been Pwned : haveibeenpwned.com

Chapitre 3.8 du rapport de l'ENISA (p. 64 à 68) à propos des fuites de données: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Notifier une violation de données personnelles auprès de la CNIL : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

SE PROTEGER DES ATTAQUES PAR REUTILISATION D'IDENTIFIANTS VOLES

Certains services, comme Dropbox, LinkedIn ou encore Adobe, ont fait l'objet de piratage et de violation massive de données à caractère personnel ces dernières années.
Les pirates ont réussi à accéder aux bases de données utilisateurs et les ont rendues publiques. Ces bases contiennent généralement les adresses email et les condensats de mots de passe. Selon les algorithmes de hachage utilisés et la complexité des mots de passe, il est possible de retrouver les mots de passe en clair.
Ces bases ayant été rendues publiques, il est possible d'y accéder et d'en obtenir une copie. Une personne malveillante pourrait donc récupérer ces identifiants afin de tenter des connexions sur d'autres services. Ces cyberattaques sont communément appelées les attaques par « credential stuffing » (réutilisation d'identifiants volés).
Voici une liste des bonnes pratiques pour se protéger de ce type d'attaque:

- **S'abonner à un service permettant d'être notifié en cas de fuite de données.** Certains sites tels que ***have i been pwned?***, regroupent les bases de données fuitées. En renseignant une adresse email, il est possible de savoir si un mot de passe associé à cette adresse a fuité et le site sur lequel il permet de se connecter. Il faut donc immédiatement changer le mot de passe sur le site correspondant. En fournissant une preuve de la responsabilité de la gestion d'un domaine, il est aussi possible d'avoir directement toutes les adresses emails du domaine concernées par des fuites https://haveibeenpwned.com/DomainSearch.
- **Utiliser des mots de passe robustes et uniques** : L'ANSSI recommande d'utiliser des mots de passe de 12 caractères avec au moins 4 familles différentes de caractère (majuscules, minuscules, chiffres, caractères spéciaux). L'utilisation de mots de passe uniques permet d'éviter que le vol d'un mot de passe donne accès à plusieurs comptes. Utiliser des mots de passe unique étant complexe, il est recommandé d'utiliser des gestionnaires de mots de passe.
- **Utiliser des gestionnaires de mots de passe**. Ces logiciels, tels que KeePass, permettent de générer des mots de passe robustes et de les stocker localement chiffrés et protégés par un mot de passe maître. Cela facilite l'utilisation de mots de passe uniques et de limiter ainsi l'impact en cas d'éventuelle fuite de données.
- **Changer de mots de passe régulièrement**. L'ANSSI recommande de changer tous les 90 jours pour les systèmes contenant des données sensibles. Cette action doit impérativement être effectuée lors d'une compromission d'un nouveau service.
- **Activer l'authentification à double facteur** : cette option disponible dans la plupart des services les plus connus (Google, Facebook, LinkedIn, etc.) permet d'ajouter un niveau de sécurité lors d'une authentification sur un nouvel appareil. En plus d'un mot de passe, le service requiert l'utilisation d'un code aléatoire à usage unique (OTP) transmis à l'utilisateur (par e-mail ou par SMS en général).
- **Prévoir des séances de sensibilisation (moodle, eformation, travaux pratiques, etc.)** : sans une sensibilisation adaptée, de mauvaises pratiques (mot de passe sous forme de post-it, stockage dans le navigateur, stockage dans un fichier texte, etc.) peuvent compromettre la sécurité des mots de passe des utilisateurs.