Prévenir une fuite de données

Une fuite de données est la divulgation non autorisée de données d'une organisation à des tiers, de manière intentionnelle ou fortuite. Les fuites de données ou exfiltration de données sont généralement la conséquence de la compromission d'un système suite à une intrusion. L'objectif de l'attaquant est de nuire à l'image de l'organisation ou d'obtenir une rançon en contrepartie de la non divulgation des données.
Elles peuvent également se produire à cause de la perte ou le vol de périphériques tels que les clés USB ou les ordinateurs portables.

Mesures de prévention

Organisationnelles

- **Classifier les données** pour mettre en œuvre le niveau de protection requis compte tenu de leur sensibilité
- **Implémenter une politique 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 alerter** en cas d'incident et **définir un plan d'action** en cas de fuite de données La réponse sera adaptée aux enjeux de la fuite (origine, données concernées, criticité...).

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

Sensibilisation

- **Promouvoir l'utilisation du chiffrement** des données sensibles lors de leur stockage et de leur transmission
- Encourager et faciliter le signalement d'activités suspectes auprès du responsable de sécurité
- **Prévoir des séances de sensibilisation** (moodle, eformation, travaux pratiques, etc.) adaptées aux profils des utilisateurs. 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.

Mesures de réaction

- **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, accident ou erreur humaine, etc.…)
- **Identifier les données qui sont ou peuvent être concernées** par la fuite en analysant les journaux d'accès des systèmes potentiellement compromis (serveur web ou frontaux, outils d'administration, applications accessibles à distance, Active Directory, etc…). En l'absence d'une expertise en interne, faire appel à un prestataire pour une analyse post-incident.
- **Notifier la direction** 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 visant à se protéger des attaques par utilisation des identifiants volés

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 les changer tous les 90 jours pour les systèmes contenant des données sensibles. Cette action doit impérativement être effectuée à la suite de la compromission d'un système.

- **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 contrôle supplémentaire 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).