Log management

Qu'est-ce que le log management ?

Le log management (**ou journalisation**) est un processus essentiel consistant à **collecter, stocker, analyser et gérer les journaux** (logs) générés par les applications, les systèmes, les serveurs, les dispositifs réseau et tout autre composant informatique d'un SI.

Une stratégie de log management efficace permet de **prévenir plusieurs risques de sécurité potentiels** :

- Elle aide à **détecter les incidents de sécurité** en analysant les modèles et les comportements anormaux dans les journaux, permettant une **réponse rapide aux intrusions**.
- Elle facilite la réalisation **d'investigations a posteriori**, en permettant de réaliser une **rétrospective des événements** afin **d'identifier les compromissions** qui ont provoquées l'incident.
- Elle contribue également à la **conformité réglementaire** en assurant la collecte, la conservation et l'analyse appropriées des journaux, ce qui **aide à prévenir les violations de données**.

Le log management appliqué à un produit peut fournir des informations sur **les tendances d'utilisation** des clients qui interagissent avec ce dernier. Ces informations peuvent être utilisées pour **optimiser le produit** ou encore **ajouter de nouvelles fonctionnalités**.

Ressources mises à disposition :

- **CLUSIF** – Référentiel des logs - Journalisation (Site Web) ;
- **ANSSI** – Recommandations de sécurité pour l'architecture d'un système de journalisation (PDF) ;
- **ANSSI** – Recommandations de sécurité pour l'architecture d'un système de journalisation en environnement Active Directory (PDF) ;
- **CNIL** – Recommandation relative aux mesures de journalisation (Site Web).

Les bonnes pratiques et mesures de sécurité :

- **Périmètre de collecte étendu :** Une journalisation étendue permet d'avoir une **visibilité complète** sur les activités se produisant dans le système.
- **Activation de l'horodatage :** L'horodatage permet **l'analyse temporelle des événements** pour reconstituer la séquence d'actions qui ont menées à un incident. Cependant, il est nécessaire que les sources de logs soient synchronisées pour permettre une corrélation correcte des événements.
- **Centralisation des logs :** En centralisant les logs, il est plus facile de **détecter les activités suspectes** et les attaques potentielles. La **corrélation des événements** provenant de différentes sources permet d'identifier les modèles de comportement malveillant.
- **Cloisonnement des serveurs de collecte :** En cloisonnant les serveurs de collecte on limite la surface d'attaque potentielle. Si un autre serveur est compromis par une attaque, cette pratique permet de **préserver l'intégrité des données de journalisation**.
- **Politique de journalisation évolutive :** Il est essentiel de faire évoluer la politique de journalisation en fonction des scénarios d'attaque. Cela permet d'améliorer la **détection de menaces** reposant sur de **nouveaux vecteurs d'attaque**.

Les points de vigilance :

Lorsque l'on manipule des données à caractère personnel il est essentiel de trouver un **équilibre entre sécurité, surveillance et risques**. Pour ce faire, il est nécessaire de prendre connaissance des **durées de rétention des journaux recommandées par la CNIL** (Site Web).