ADMINISTRATION

Audit et contrôle | ADMI04

Contexte :

Cette activité repose sur l'analyse et les diagnostics incluant l'exploitation des fichiers journaux (en supposant que toutes les démarches prévues par la loi ou le cadre d'utilisation ont été effectuées), des registres de suivi, des recueils manuscrits.

Objectifs :

Identifier les dysfonctionnements et proposer des actions d'amélioration :

- Déterminer *a posteriori* si des tentatives d'atteinte au système d'information ont eu lieu: intrusion, altération de données, utilisation abusive ou aberrante.
- Vérifier l'efficacité des moyens de sécurité mis en place.
- Déterminer les performances des réseaux et des systèmes.
- Vérifier que les normes, consignes sont bien appliquées.
- Élucider des problèmes techniques…

Recommandations :

La mise en œuvre d'un audit s'appuie sur les responsables locaux, les responsables réseaux et bureautiques, ainsi que sur les méthodes et outils informatiques existants (cf. par exemple la méthode « MEHARI » du CLUSIF). Pour être efficace, l'audit doit prendre en compte l'intégralité du système d'information.

Une périodicité de déclenchement des audits sera définie et mise en application pour chaque nouveau réseau ou extension importante d'un réseau existant.

Le responsable sécurité, en relation avec la direction concernée, est chargé de définir le cadre de l'audit et les conditions de sa mise en oeuvre. Le service informatique et les responsables locaux sont responsables de la mise en place des actions correctives en respectant la propriété des données.

L'analyse « manuelle » des fichiers journaux nécessite beaucoup, voire énormément de temps. Pour qu'elle soit pertinente, on doit l'effectuer selon une périodicité correctement choisie en fonction du volume de données à analyser

On peut utiliser le cas échéant des outils d'analyse automatique, s'ils existent pour le type d'informations considéré.

Dans le cas de vérification de l'application des consignes ou procédures, on effectuera de préférence des contrôles impromptus.