Formation F02

Comment réaliser l'audit sécurité de votre système d'information

Plan détaillé de la formation

--- 1° jour --->

Introduction

- Objectif de cette formation.
- Où se situe l'audit de sécurité dans le cadre d'une « démarche sécurité globale » ?
- Qu'est-ce qu'un audit de sécurité du système d'information ?
- Où se situe l'audit de sécurité dans la politique de sécurité informatique et informationnelle ?
- Quelle est votre responsabilité ?

I. Comprendre l'audit sécurité

1. Comment organiser et mener un audit de sécurité
   - Quelle est l'origine de cet audit ?
   - Quels sont les objectifs de cet audit ?
   - Déterminer le périmètre de cet audit.
   - Les facteurs clé de réussite d'un audit.
   - Suivre le fil rouge.
   - Organiser les entretiens.
   - Les qualités de l'auditeur.

2. La démarche sécurité
   - Le cycle « Réflexion --> Action --> Controle ».
   - La Politique de Sécurité Informatique et Informationnelle (PSII).
   - Un exemple de PSII en 10 étapes (incluant l'audit sécurité).
   - Les étapes de l'audit sécurité.
   - Comment rédiger le rapport d'audit sécurité ?

3. Les pré-requis **indispensables** (la collecte préalable des informations)
   - Décrire ou obtenir la description du système d'information concerné par l'audit sécurité (périmètre). Modélisation.
   - Décrire ou obtenir la description des relations (points d'entrée/sortie, flux) de ce système d'information avec l'extérieur. Modélisation.
   - Classifier ou obtenir la classification des biens à protéger.

--- 2° jour --->

II. Réaliser l'audit de sécurité

1. Recenser et évaluer
   - Les menaces potentielles et le degré de sensibilité de l'Organisation et de son système d'information.
   - Les menaces avérées et le degré d'exposition de l'Organisation et de son système d'information.
   - Les incidents et les attaques connues, les incidents et les attaques possibles et le degré de vulnérabilité du système d'information de l'Organisation.
   - Les dégâts subis par le système d'information et son degré de *dommageabilité*.
   - Les actions de réparation et de compensation entreprises suite à ces dégats et la capacité de récupération du système d'information.

2. Analyser
   - Evaluer la Politique de Sécurité Informatique et Informationnelle existante.
   - Evaluer les moyens de protection existants pour assurer la sécurité du système d'information de l'Organisation.
   - Evaluer l'implication des acteurs du système d'information sur le plan de la sécurité.
   - Estimer le poids de la contrainte sécurité par rapport à l'exploitation souhaitée du système d'information.
   - Synthèse des problèmes de sécurité posés par le système d'information de l'Organisation.

3. Concevoir et rédiger les premières recommandations
   - Rappeler l'ensemble des attaques possibles contre le système d'information et sélectionner les plus critiques.
   - Proposer des moyens de détecter, de déjouer (ou de neutraliser) et d'atténuer ces attaques.
   - Définir les objectifs de sécurité à atteindre.
   - Définir les fonctions de sécurité à mettre en œuvre et leur niveau souhaitable.

Conclusion

- Pas d'audit de sécurité sans simplicité et clarté.
- Pas d'audit de sécurité sans démarche et méthode.
- Un audit de sécurité ne sert à rien sans intégration dans une politique de sécurité.
- La nouvelle approche de la sécurité doit être globale (informatique et informationnelle).
- Pas d'audit de sécurité sans l'implication des personnels de l'Organisation auditée.

<--- Fin de la formation ---