Formation F03

Comment élaborer votre politique de sécurité informatique et informationnelle (PSII)

Plan détaillé de la formation

--- 1° jour --->

Introduction

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

I. Comprendre la politique de sécurité

1. Comment élaborer une politique de sécurité
   - Quelle est l'origine de cette mission ?
   - Quels sont les objectifs de cette politique de sécurité ?
   - Déterminer le périmètre de cette politique de sécurité.
   - Les facteurs clé de réussite d'une politique de sécurité.
   - Suivre le fil rouge.
   - Les qualités du RSSI ou du consultant en charge de cette élaboration.

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 la politique de sécurité.
   - Comment rédiger la politique de sécurité ?

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

--- 2° jour --->

II. Elaborer la politique de sécurité

Phase 1 - Réflexion : Audit sécurité

1. Décrire et modéliser le système d'information concerné par la politique de sécurité

2. 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.

3. 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.

4. 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.

--- 3° jour --->

Phase 2 - Action : Conception, réalisation et mise en oeuvre des solutions de sécurité et management de la sécurité

5. Concevoir les solutions de sécurité.

6. Recenser et choisir les outils de sécurité nécessaires aux solutions.

7. Installer et mettre en œuvre les dispositifs de sécurité.

8. Définir les procédures de sécurité.

9. Définir les règles de sécurité au sein de ces procédures.

10. Définir et attribuer un rôle précis à chacun des intervenants dans la sécurité.

11. Informer les intervenants et les utilisateurs.

12. Former les intervenants et les utilisateurs.

13. Reporter à la Direction Générale.

Phase 3 - Contrôle : Contrôle, mesure et évolution de la sécurité

14. Contrôler les résultats obtenus par rapport aux objectifs fixés.

15. Faire évoluer le système de sécurité en phase avec l'évolution du système d'information.

Conclusion

- Pas politique de sécurité sans simplicité et clarté.
- Pas politique de sécurité sans démarche et méthode.
- La nouvelle approche de la sécurité doit être globale (informatique et informationnelle).
- Pas de politique de sécurité sans l'implication des personnels de l'Organisation.

<--- Fin de la formation ---