Méthodes de lutte contre la fraude informatique

Les moyens des fraudeurs se multiplient avec l'évolution des techniques. Il est de plus en plus difficile, sans avoir des connaissances suffisantes, de déterminer rapidement les faiblesses d'une organisation, et trouver les parades adaptées.

Objectifs :

- Donner une vision globale de la fraude et de ses implications,
- Permettre aux auditeurs de réagir suffisamment vite et de conseiller les décideurs sur les dispositifs de sécurité à mettre en œuvre pour éviter les fraudes,
- Identifier les points-clés de la démarche d'audit appliquée à la détection des fraudes.

Participants :

Auditeurs, consultants, responsables sécurité des systèmes d'information, risk managers, responsables informatiques

Prérequis :

Connaissances générales concernant l'informatique et notamment les communications.

Programme détaillé :

1ère partie – La fraude classique

- Définitions et inventaires – L'arbre des fraudes
- « Quid » de la fraude
- Caractéristiques de la fraude
- Buts recherchés
- Environnement de la fraude
- Les supports de la fraude
- La méthode applicable
- La mécanisation des recherches
- Les aspects juridiques

2ème partie – La fraude informatique

- Les réseaux
- Les communications
- Internet – Intranet – Extranet
- L'administration de la sécurité
- La piste d'audit adaptée à l'informatique
- Les grands classiques informatiques
  - La fraude applicative
  - La fraude à partir du système d'exploitation
  - La fraude en production
  - La fraude via les réseaux
  - Le « craquage » des mots de passe
- Quelques spécificités
  - Fraude sur les ERP (achats et ventes),
  - Fraudes sur cartes bancaires
  - Les « pourriciels »

1ère Etude de cas : « le salami »

- Les cyber fraudes
- Le « sniffing »
- Le « spoofing »
- Le chantage aux fichiers cryptés (technique PGPxx)
- Le « flooding »
- Le « TCP-SYN Flooding »
- Le « smurf »
- Le débordement de tampon
- Les virus, vers, chevaux de Troie
- Les bombes logiques
- Les « hoax »
- Les « backdoors »
- L'ingénierie sociale
- Mascarade et pirata ge de sites…
- Autres aspects de la fraude informatique
  - La technique dite du Salami

- Le piratage de logiciels
- Les logiciels d'attaque et de piratage
- Captage et découplage…

3ème partie – Méthode de lutte contre la fraude informatique – Indicateurs

- Indicateurs
- Les contrôles (accusés réception automatiques,…)
- Les liens entre cartographie applicative, cartographie des risques, cartographie des réseaux
- Les « règles du jeu »
- L'obligation d'inventaire des contrôles automatisés
- La séparation des tâches informatiques (la matrice des habilitations)
- Benford
- La cryptologie et la cryptanalyse

2ème étude de cas : Matrice des habilitations

- La documentation – sa conservation (historisation)
- Protection des sauvegardes
- Les fiches techniques de détection et prévention de la fraude (FTDF)

3ème Etude de cas – Etablissement d'une FTDF fraude informatique

4ème partie – Les auditeurs et la gestion de la fraude

- Les points d'accroche
- Méthodologie
- 1ère phase : Identification – qualification – recherches complémentaires – coûts financiers
- 2ème phase : Analyse et coordination
- 3ème phase : Communication et rapport

Conclusion – Stratégie de lutte contre la fraude

- Lutte contre les pourriciels et la manipulation des comptes,
- La place des auditeurs dans la stratégie de lutte,
- Le rôle du secteur « risk management »,
- Le rôle des autres organes de l'entreprise,
- L'excellence du contrôle interne classique et informatisé.

Durée : 2 jours

Référence : FAS001