Cybersécurité : Etat de l'art - principes et notions fondamentales de la sécurité des systèmes d'information

Objectifs / Durée de la formation

Durée: 5 jours, soit 35 heures

- Comprendre les menaces sur les équipements de l'infrastructure
- Mettre en place une politique interne (technologique et humaine) de sécurité des informations
- Choisir les dispositifs et emplacements de sécurité
- Concevoir le Plan de Sécurité
- Connaître le vocabulaire et les principes théoriques de la sécurité des systèmes d'information, mais de manière très pratique, donc très concrète, pour des praticiens
- Connaître toutes les base de la sécurité opérationnelle, à la fois en sécurité réseau, en sécurité des systèmes Windows et Linux et en sécurité applicative

Participants / Pré-requis

- DSI, RSSI, RSI, Technicien sécurité
- Administrateurs systèmes et réseaux, responsables informatique et/ou sécurité
- Une réelle connaissance informatique est nécessaire

Moyens pédagogiques

- Formateur expert dans le domaine
- Mise à disposition d'un ordinateur, support de cours remis à chaque participant, vidéo projecteur, tableau blanc et paperboard
- Feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation, questionnaire de satisfaction, attestation de stage

Programme

1. Domaines et contours de la sécurité

- Les systèmes de gouvernance
- Présentation des risques involontaires
- Cybercriminalité
- Le cycle de la gouvernance
- Les organes de contrôle
- Le contrôle Interne
- Les audits externes
- Les acteurs de la sécurité
- Environnement juridiques
- Droits et obligations des entreprises en termes de sécurité
- La loi Sécurité Financière SOX (Sarbane Oxley) , La CNIL

2. Analyse des risques

- Connaître son SI
- PC final
- Serveur
- Utilisation d'une ferme de serveurs
- Quelles sont les données externalisées (cloud) ?
- Matériel réseau
- Méthodes d'accès aux réseaux
- Méthodes d'identification
- Gestion des autorisation
- Risques de piratage
- Risques de perte d'information
- Risques de vols d'information
- Risques naturels
- Les pannes matérielles
- Les risques d'ingénierie sociale

3. Mise en oeuvre d'une politique de sécurité

- La sécurité physique
- Accès aux installations
- Sécurité des installations (incendies, inondations, vols...)
- Prévision d'un plan de continuité et de reprise
- Contrôler les accès
- La sécurité des services
- Sécuriser les applications
- Cryptage
- Technologies VPN
- VPN SSL
- HTTPS
- Sécurité des protocoles Peer-to-peer
- Blocage des applications
- Sécurité des terminaux mobiles
- Utilisation d'une DMZ
- Comment intégrer la disponibilité et la mobilité des collaborateurs
- Généralités sur les outils disponibles

4. Les aspects organisationnels de la sécurité

- Définition des risques
- Confidentialité
- Intégrité
- Supervision
- La veille technologique
- Publication des failles
- Principe du modèle de maturité
- Sécurité du système d'exploitation
- Gestion des privilèges
- Documentation

5. Management de la sécurité

- Les méthodes Méhari EBIOS ISO 27001 Cobit
- Les limites de ces méthodes
- Les audits de sécurité
- Mener un audit dans une entreprise multisites

- Trop de sécurité tue la sécurité, comment éviter les faux-positifs
- Expliquer les enjeux de la sécurité aux utilisateurs finaux et aux directions
- La roue de la sécurité
- Mise en oeuvre technique de la sécurité
- Stress du système
- Amélioration de la sécurité
- Savoir protéger les investissements au meilleur coût pour les meilleures raison
- Communications sur la politique de sécurité
- Comment réagir à une attaque (en interne, en externe)
- Les limites du plan de sécurité et les dispositions juridiques
- Définition et rôle du RSSI

6. Méthodologie et technologie

- La vision de la sécurité selon les interlocuteurs
- Les objectifs
- Les moyens techniques et financiers mis en oeuvre
- La stratégie
- L'adaptation et la gestion du changement
- Elaboration du plan de sécurité
- L'audit de conformité
- Les indicateurs
- Les tableaux de bords à établir
- Les méthodologies d'audit

7. Les outils

- Fonction d'un firewall
- Documentation des accès autorisés sur le réseau
- Création d'une charte d'utilisation du réseau pour les collaborateurs
- Fonction d'un système de détection d'intrusion
- Les logiciels clients de sécurité (firewall, antivirus, antispyware...)
- Superviser la sécurité
- Faire évoluer la sécurité
- Contraction d'assurances : quelles sont les garanties ? qu'est ce qui peut et doit être assuré ? l'importance de la disponibilité du système
- Validation technique de l'architecture
- Formation des personnels du SI
- Formation des utilisateurs du SI
- Avenir de la sécurité informatique
- Les 6 idées les plus stupides selon Marcus J. Ranum
- La vision géostratégique de la sécurité
- Les phénomènes de monopole

8. Rédaction de chartes d'utilisation et / ou de configuration

- Le secret professionnel
- Le respect de la législation
- Les règles de confidentialité
- L'usage des services Internet
- Définir sa charte d'utilisation
- Responsabilités du comité de coordination du SI
- Responsabilités du conseil d'administration et des représentants

9. Concepts de base des réseaux

- Paquets et adresses

- Ports de services IP
- Protocoles sur IP
- TCP / UDP / ICMP
- DHCP / DNS
- VoIP (SI P)
- Réseaux sans fil

10. Sécurité physique

- Services généraux
- Contrôles techniques
- Menaces sur la sécurité physique

11. Principes de base de la SSI

- Modèle de risque
- Défense en profondeur
- Identification, authentification et autorisation
- Classification des données
- Vulnérabilités

12. Politiques de sécurité informatique

- Principe
- Rôles et responsabilité

13. Plan de continuité d'activité

- Exigences légales et réglementaires
- Stratégie et plan de reprise après sinistre

14. Analyse des conséquences

- Évaluation de crise
- Facteurs de succès
- Fonctions business critiques

15. Gestion des mots de passe

- Stockage, transmission et attaque des mots de passe Windows
- Authentification forte (Tokens, biométrie)
- Single Sign On
- RADIUS

16. Sécurité Web

- Protocoles de sécurité du Web
- Contenus dynamiques
- Attaques des applications Web
- Durcissement des applications Web

17. Détection d'intrusion en local

- Détection d'intrusion
- A quoi s'attendre

18. Détection d'intrusion en réseau

- Outils
- Déni de service
- Réaction automatisée

19. Pots de miel

20. Gestion des incidents de sécurité

- Préparation, identification et confinement
- Eradication, recouvrement et retour d'expérience
- Techniques d'enquête et criminalistique informatique

21. Guerre de l'information offensive et défensive

22. Méthodes d'attaques

- Débordement de tampon
- Comptes par défaut
- Envoi de messages en masse
- Navigation web
- Accès concurrents

23. Pare-feu et zones de périmètres

- Types de pare-feu
- Architectures possibles : avantages et inconvénients

24. Audit et appréciation des risques

- Méthodologies d'appréciation des risques
- Approches de la gestion du risque
- Calcul du risque / SLE / ALE

25. Cryptographie

- Besoin de cryptographie
- Types de chiffrement
- Symétrique / Asymétrique
- Empreinte ou condensat
- Chiffrement
- Algorithmes
- Attaques cryptographiques
- Types d'accès à distance (VPN, DirectAccess)
- Infrastructures de Gestion de Clés
- Certificats numériques
- Séquestre de clés

26. PGP

- Installation et utilisation de PGP
- Signature de données
- Gestion des clés
- Serveurs de clés

27. Stéganographie

- Types
- Applications
- Détection
- Exigences légales
- Gestion administrative
- Responsabilité individuelle
- Opérations privilégiées
- Types de mesures de sécurité
- Reporting