Audit sécurité des systèmes d'information

- Informatique - Sécurité Informatique -

Date de mise en ligne : samedi 4 novembre 2006

Spyworld Actu

Les objectifs de la formation

- Identifiez vos objectifs et obligations en matière de sécurité informatique
- Structurez toutes les étapes de votre audit sécurité et intégrez les principaux référentiels
- Réalisez le plan d'actions correctives de votre politique sécurité

Calendrier des sessions

- du 07 au 08 Décembre 2006
- du 08 au 09 Mars 2007
- du 13 au 14 Juin 2007

Tarifs Journées Formation (2 jours) : 1645 euros HT

Vous êtes concerné

- Responsable de la Sécurité des Systèmes d'Information
- Directeur des Systèmes d'Information
- Responsable informatique
- Directeur technique
- Responsable de l'Audit Informatique
- Responsable de l'exploitation
- Gestionnaire de risques
- Auditeur informatique
- Responsable des réseaux
- Chef de projet informatique
- Auditeur en SSII
- Consultant

Le programme détaillé

PROGRAMME DU PREMIER JOUR

8h45 : Accueil des participants

Loi informatique et Liberté, SOX, LSF... Identifier vos obligations et contraintes liées au nouveau contexte juridique de la sécurité informatique

- Vers une obligation générale de sécurité des données : Loi informatique et Liberté, Décret Code des marchés publics, LSF, SOX...
- La responsabilité des dirigeants, des RSSI, des utilisateurs
- Quelle est la responsabilité du prestataire de services en matière de solutions de sécurité ? Les problèmes propres à l'infogérance
- Quels sont les droits des RSSI en matière de contrôle de l'activité des salariés ? L'élaboration des chartes
- Les principes de la signature électronique

PREPARER ET ORGANISER VOTRE AUDIT SECURITE

Fixer les objectifs de votre audit de la sécurité de vos Systèmes d'Information

- Les différents audits pour analyser le niveau de sécurité de votre entreprise : les audits de sécurité, les audits applicatifs...
- Appréhender les préoccupations de la direction pour mieux y répondre, les principaux risques
- Définir l'objet de votre mission, le périmètre et les destinataires de vos analyses : évaluation de la politique de sécurité, test d'intrusion...
- Quelle démarche ? Quelles méthodes et quels référentiels utiliser ? Quels résultats ?
- Quels risques issus de votre démarche ?

Comment identifier le patrimoine informationnel de votre entreprise à protéger en priorité ?

- Identifier les données sensibles de l'entreprise, les applications stratégiques vis à vis de son coeur de métier...
- Comment procéder à la classification des ressources par niveau de sensibilité ?
- Confidentialité, intégrité, disponibilité, authenticité, traçabilité... Définir les objectifs incontournables de la sécurité de votre entreprise

Déjeuner d'échanges

STRUCTURER VOTRE DEMARCHE D'AUDIT POUR ÉVALUER VOTRE SYSTÈME DE SÉCURITÉ INFORMATIQUE ET AJUSTER VOS INVESTISSEMENTS

ISO 17799, COBIT, ITIL... Quels atouts et limites des référentiels à la mode ? Comment les mettre en oeuvre simplement ?

- Panorama des référentiels existants, objectifs, points forts et limites : ISO 17799, ISO 27001, BS 7799, Méthode EBIOS, Méthode MEHARI, Méthode PDCA, COBIT, ITIL, CMMi...
- Comment adapter un référentiel aux objectifs de votre audit ? L'exemple avec COBIT
- Le point sur les offres des sociétés spécialisées en matière d'assessment et d'audit de l'environnement de sécurité

Les dangers qui menacent votre entreprise en 2006 : Quels outils et techniques d'identification ? Quels impacts d'une sécurité défaillante ?

- Les menaces connues, potentielles et subies par votre entreprise et leurs évolutions en 2006 : vol ou altération d'information, intrusions...
- Diagnostic et analyse : les techniques, outils et logiciels à votre disposition
- Identifier les facteurs de limitation des risques et les facteurs aggravants : management non sensible, nomadisme important, sites marchands, compétence du personnel...
- Impact financier, pénal, remise en cause des contrats d'assurance, perte d'image, perte d'information, perte d'exploitation... Comment estimer les préjudices et les pondérer ?
- Déterminer le degré d'exposition de l'entreprise et de son SI, sa vulnérabilité, sa capacité de compensation et de récupération

Cas pratique

Cas pratique : DG, DSI, RSSI, consultants... Construire la matrice des acteurs de la sécurité pour analyser l'efficacité de votre organisation

Les participants établissent la liste des acteurs de la sécurité, et définissent les rôles et responsabilités de chacun. Avec l'aide du formateur, ils construisent ensuite leur matrice organisationnelle pour identifier certaines incompatibilités et valider la correcte séparation des tâches. Indispensable dans les grandes entreprises, l'intervenant adapte également cet exercice au contexte des PME.

PROGRAMME DU DEUXIEME JOUR

8h45 : Accueil des participants

Evaluer les moyens de protection existants pour assurer la sécurité du Système d'Information

- Evaluation de votre PSI : politique, organisation et administration de la sécurité
- Sécurité logique, Internet, du réseau et des télécommunications... Comment faire le point sur chaque domaine d'application de votre stratégie de sécurité ? Quels critères d'évaluation de la sécurité ?
- Les risques particuliers liés à Internet et au sans fil, les menaces les plus courantes
- Quel poids de la contrainte sécurité sur l'efficacité souhaitée dans l'utilisation de vos SI ?

Quelle démarche appliquer pour l'audit du plan de continuité d'activité ?

- Comment analyser, tester et maintenir votre plan de continuité de l'activité ?
- Les différentes stratégies d'un plan de reprise informatique
- Comment évaluer l'implication du personnel de l'entreprise ?

Cas pratique

Cas pratique : Analyser la valeur et les limites pour l'entreprise d'une solution centralisée de sécurité logique

L'entreprise de distribution X est confrontée à une multitude d'applications. Elle constate une baisse de productivité et a des soupçons de fraude interne. Les participants réalisent le calcul du ROI d'une solution d'authentification forte de type « Single Sign On » basé sur un annuaire interne LDAP.

Cas pratique

Cas pratique : Construire votre check-list d'autoévaluation de la sécurité de votre entreprise

Déjeuner d'échanges

FIXER VOS AXES D'AMELIORATION ET BATIR VOTRE PLAN D'ACTION

Comment faire évoluer votre politique de sécurité pour réduire les risques en cohérence avec les besoins de votre organisation ?

- Définir les objectifs et les fonctions de sécurité à atteindre et à mettre en oeuvre
- Faire le point sur les faiblesses de la sécurité des SI révélés par votre audit
- Définir vos priorités concernant les moyens de protection et les grands axes des solutions de sécurité à mettre en oeuvre
- Réaliser un transfert de risque vers l'assurance : comment identifier et définir ce qui est assurable pour l'entreprise ? Les limites du transfert en cas de crise grave

Cas pratique

Cas pratique : Concevoir un plan d'actions correctives réaliste : quelles méthodes ? Quels outils ?

Après une intrusion par des hackers sur le site Internet, les participants analysent les failles de l'architecture existante et établissent une architecture de sécurité pour l'entreprise X qui a besoin d'un espace intranet pour ses collaborateurs, d'un espace Internet pour ses clients et d'un espace extranet pour ses partenaires. Ils positionnent les différents dispositifs (firewall, proxy, routeurs...) en fonction de leurs caractéristiques et des besoins réels de l'entreprise.

Les outils pour capitaliser sur votre audit et communiquer avec la Direction Générale

- Reportings sécurité, comités de pilotage, alertes... Quelles informations privilégier ?
- Quels indicateurs de suivi mettre en oeuvre ? Comment les intégrer dans vos relations fournisseurs ?
- Les points de contrôles à mettre en place pour tout nouveau projet
- Utiliser des tableaux de bord organisationnels et techniques compréhensibles par le top management
- Comment justifier des investissements ? Communiquer un message positif

Post-scriptum :

http://www.comundi.fr/forma-inter/6...