Formation Devenir Responsable de la Sécurité du Système d'Information

La sécurité informatique revêt aujourd'hui une telle importance que les responsables de la sécurité des systèmes d'information sont couramment rattachés aux directions générales des entreprises. La mission du RSSI est effectivement essentielle puisqu'il a la charge des choix et des actions relatives à la sécurité des systèmes, des réseaux, des applications et des données de l'entreprise

Objectifs

- Identifier toutes les facettes du métier de Responsable de la Sécurité du SI
- Être en mesure d'évaluer les risques encourus par son système d'information et d'engager les actions nécessaires
- Savoir construire une politique de sécurité efficace
- Comprendre l'importance des plans de continuité et de secours et être capable de les mettre en place

Public concerné

- Responsables ou directeurs informatique souhaitant évoluer vers le métier de RSSI
- RSSI opérationnels souhaitant appréhender les nouvelles missions du RSSI
- Dirigeants et cadres souhaitant acquérir une meilleure compréhension des enjeux de la sécurité et d

Prérequis

- Bonne culture générale sur les infrastructures IT

Une formation de 6 jours

Caractéristiques
Tarif : 3490 euros HT par personne
Numéro de formateur : 11754730575
Nombre d'heures : 42
Référence : MG802
Contact : Jean JUILLET
Telephone : 01.42.62.91.86
Email : contact@kaptive.com

Paris
06/01/2014
27/01/2014
10/03/2014
21/03/2014
02/06/2014
23/06/2014
01/09/2014
22/09/2014
24/11/2014

Lyon
03/02/2014
24/02/2014
26/05/2014
16/06/2014
29/09/2014
20/10/2014

Description des modules

1ere partie : Le métier de RSSI, son rôle, ses responsabilités, son périmètre d'action et ses méthodes de travail

Introduction : Quels sont les enjeux de la SSI ? Pourquoi mettre en place des politiques de sécurité des SI ?

- Quelques définitions et terminologies de base : - définition de l'information (I) - définition de la protection de l'information (PI) - définition du système d'information (SI) - définition de la sécurité du système d'information (SSI)
- Les enjeux de la sécurité de l'information : - L'environnement concurrentiel - Les risques de dysfonctionnement des processus critiques - Les risques juridiques
- La nature des menaces et des risques : - Les risques relatifs aux processus métiers - Les risques relatifs aux ressources humaines - Les risques relatifs aux moyens logistiques - Les risques relatifs aux systèmes informatiques - Les risques relatifs aux partenaires - Les catégories de menaces (accidents, erreurs, malveillances) - La gestion des risques
- L'évolution de la maturité des entreprises en SSI : - La maturité technologique - La maturité organisationnelle - La maturité décisionnelle
- Les enjeux juridiques et réglementaires : - 40 ans d'histoire - Les obligations légales et les directives internationales (OCDE, CE, ..) - La loi informatique et libertés - Le RGS 1.0, son contenu et ses objectifs
- Les exigences de sécurité : - Les exigences en matière de disponibilité - Les exigences en matière d'intégrité - Les exigences en matière de confidentialité - Les exigences en matière de traçabilité

Gouvernance de la SSI : Quel est le rôle du RSSI ?

- La gouvernance générale de la SSI, les rôles et les responsabilités : - Rôle de la maitrise d'ouvrage - Rôle de la maitrise d'oeuvre - Rôle de la direction générale - Rôle de l'audit et du contrôle interne - Rôle du CIL et du RSSI - Rôle des utilisateurs - Rôle de la DSI
- Le métier de RSSI : - RSSI MOA vs RSSI MOE - son positionnement, son profil et sa fiche de poste - Le rôle et les responsabilités du RSSI

Mettre en oeuvre une gestion structurée de la sécurité (SMSI)

- Pourquoi mettre en oeuvre un système de management de la SSI : - Définition d'un système de management de la sécurité de l'information (SMSI) - le SMSI et les autres systèmes de management l'historique et l'origine des normes ISO 27000 les arguments pour la mise en oeuvre d'un SMSI toutes les normes de la filière ISO 27000 le processus de certification
- Présentation des normes ISO27001 : - la structure documentaire de la norme ISO 27001 - description du processus d'amélioration continue - les exigences de la phase « Pan » - les exigences de la phase « Do » - les exigences de la phase « Check » - les exigences de la phase « Act » - les exigences relatives à la documentation du SMSI - la responsabilité de la Direction Générale - l'audit et la révision du SMSI
- Présentation des normes ISO27002 : - la structure documentaire de la norme ISO 27002 - les directives relatives à la politique de la sécurité de l'information - les directives relatives à l'organisation de la sécurité de l'information - les directives relatives à la gestion des biens - les directives relatives à la sécurité liée aux ressources humaines - les directives relatives à la sécurité physique et environnementale - les directives relatives à la gestion et l'exploitation des télécommunications - les directives relatives au contrôle d'accès - les directives relatives à l'acquisition, le développement et la maintenance des systèmes d'information - les directives relatives à la gestion des incidents de sécurité de l'information - les directives relatives à la gestion du plan de continuité d'activité - les directives relatives à la conformité
- Les conseils de mise en oeuvre d'un SMSI

Comment évaluer les risques dans son système d'information ?

- Concepts fondamentaux d'analyse des risques : - les risques bruts vs les risques nets - les typologies de menaces - les vulnérabilités techniques et organisationnelles - les notions de dégâts et d'impacts - les métriques de mesures des risques - les approches qualitatives vs quantitatives
- Panorama des méthodes et des normes du marché : - historiques de méthodes et des normes relatives à la gestion des risques - présentation du guide 73 : 2009 - présentation de la norme ISO 27005 :2008 - présentation de la norme ISO 31000 :2009 - présentation de la démarche FERMA - présentation de la méthode EBIOS (ANSSI) - présentation de la méthode MEHARI (CLUSIF)
- Les conseils de mise en oeuvre d'une gestion structurée des risques : - le système de management des

risques - la gouvernance à mettre en oeuvre - les acteurs leur rôle et responsabilité

Introduction aux plans de continuité des activités et plans de secours

- Fondamentaux de la continuité des activités : - définition de la continuité d'activité - les enjeux en matière de continuité d'activité - les normes en vigueur (BCI, BS25999, ...) - l'évaluation des BIA et des risques
- Les différents plans et leur mise en oeuvre : - le plan de continuité des opérations métiers (PCO - le plan de repli et d'hébergement des utilisateurs (PHEB) - le plan de gestion de crise et de communication - le plan de secours informatique - le plan de formation des utilisateurs, des acteurs de la crise et des MOE - le plan de test du PCA - le maintien en condition opérationnelle du PCA (MCO)
- Le modèle du BCI et de la norme BS25999 : - les modèles proposés - le processus d'amélioration continue
- Les phases d'un projet de PCA : - les 5 phases de la construction d'un PCA - la gouvernance de projet vs la gouvernance du PCA - la conduite de projet et la gestion documentaire - la conduite du changement - le rôle du management dans la conduite du projet
- Les outils logiciels disponibles sur le marché

2ème partie : de la théorie à la pratique

Construire sa politique de sécurité

- Structure et acteurs d'une politique de sécurité : - les rôles et les responsabilités dans la définition de la politique de sécurité - la gouvernance à prévoir - la structure documentaire à prévoir - la prise en compte des autres politiques de sécurité internes à l'entreprise
- Comment définir sa politique générale de sécurité et les politiques spécifiques qui en découlent : - le contenu d'une politique générale de sécurité de l'information - le contenu d'une politique spécifique de sécurité informatique - le contenu d'une politique spécifique de sécurité relative à la protection des données à caractère personnel - le contenu d'une politique spécifique de sécurité relative à la gestion des journaux informatiques - le contenu d'une politique spécifique de sécurité relative à la sécurité physique
- Comment construire la charte utilisateurs : - objectifs et finalité de la charte - les acteurs impliqués dans la construction de la charte - le contenu d'une charte - la diffusion de la charte
- Sensibilisation et responsabilisation des utilisateurs : modifier les comportements : - les acteurs de la sensibilisation - les méthodes de sensibilisation - l'e-learning sécurité, apport et solution
- Communiquer et diffuser la politique de sécurité : les bonnes pratiques

L'état de l'art et du marché des solutions technique de sécurité

- La sécurité physique des ressources informatiques : - La protection contre les incendies - La protection contre les vols - La protection contre les dégâts des eaux - La protection contre la chaleur - La protection de l'environnement de travail des utilisateurs
- La sécurité dans les réseaux et télécoms : - Les composants de sécurité (FW, IDS/IPS, Proxy, ...) - Les typologies d'architecture - Les VNP - La sécurité des postes de travail mobiles
- La sécurité dans les systèmes et les applications : - Les contrôles d'accès aux systèmes et applications -La gestion des filtrages -Confinement des environnements -Sécurité de l'architecture -Gestion et enregistrement des traces -Protection des accès logiques -IAM -authentification forte -SSO -One time Password
- La sécurité des postes de travail et des outils de mobilité : - Protection de l'environnement de travail - Authentification forte et chiffrement - Les solutions VPN - La lutte anti virale - Cas particulier des mobiles phones

Construire son plan d'action sécurité

- Concevoir sa stratégie sécurité : - Le schéma directeur SSI - Le plan de prévention des risques (PPR) - Les coûts d'investissement vs les coûts d'exploitation - Les retours sur investissements - La gouvernance à prévoir pour la définition et la validation
- Sélectionner les mesures de maîtrise des risques : - Les projets de sécurité à prévoir - Les mesures de sécurité et leur priorité - Les acteurs de la maitrise d'oeuvre - La mise en oeuvre au travers de FTMO
- élaborer un plan d'action pluriannuel : - Exemple de schéma directeur pluriannuel - Le maintien en condition opérationnel du SDSSI
- Les arguments pour convaincre la direction générale et les équipes de maitrise d'oeuvre

élaborer un tableau de bord de restitution en Direction générale

- Méthodologie et démarche : - La méthode proposée par l'ANSSI - La gouvernance lors de l'élaboration des tableaux de bord - Les groupes de travail à prévoir - La structure du tableau de bord - Les tableaux de bord décisionnels - Les tableaux de bord tactiques - Les tableaux de bord opérationnels

- Définition des indicateurs de sécurité : - La collecte des besoins - La liste des indicateurs (exemple basé sur des cas pratiques) - L'analyse de faisabilité technique de remontée des indicateurs
- Formalisation et mise à jour des tableaux de bord : - Le formalisme attendu par les destinataires des tableaux de bord - La fréquence d'alimentation des tableaux de bord - La diffusion des tableaux de bord - Le maintien en condition opérationnelle des tableaux de bord - Les outils de pilotage et de suivi des tableaux de bord

Conseils généraux pour réussir dans son métier de RSSI

- Les freins et les difficultés rencontrés par les RSSI (retour d'expérience)
- La bonne appropriation et la bonne communication du rôle du RSSI
- La boîte à outil indispensable du RSSI
- Les erreurs à ne pas commettre, les conseils d'accompagnement au changement
- Les relais d'information du RSSI
- Les outils pédagogiques