Formation Sécurité Informatique pour Non-Informaticien : Vocabulaire, Concepts et Technologies

Objectifs de la formation Sécurité Informatique pour Non-Informaticien

Si, aujourd'hui, bon nombre d'utilisateurs perçoivent l'importance de la sécurité des appareils informatiques et des données, en comprendre les mécanismes et les outils semble inaccessible aux non-spécialistes.
Ce séminaire "Sécurité informatique pour non-informaticiens" vous explique les concepts, le vocabulaire et les moyens disponibles pour la mettre en œuvre. Il vous apprend les bases qui vous permettront de communiquer et collaborer avec les équipes internes, les prestataires ou les fournisseurs spécialisés.

À l'issue de cette formation, vous aurez acquis les connaissances nécessaires pour :

- Comprendre les concepts en matière de sécurité informatique, les technologies actuelles et les solutions utilisées
- Connaître le rôle et le métier des acteurs du marché
- Avoir une vision globale de la sécurité informatique afin de dialoguer avec les professionnels et piloter les prestataires
- Identifier les nouveaux enjeux associés à la sécurité informatique

À qui s'adresse cette formation ?

Public :

Cette formation "Sécurité informatique pour non-informaticiens" s'adresse aux professionnels amenés à évoluer dans l'univers de la sécurité informatique : commerciaux, marketeurs, consultants, chefs de projets, responsables de formation, et à toute personne souhaitant comprendre la sécurité informatique.

Prérequis :

Ce séminaire sur la sécurité informatique ne nécessite pas de connaissances en informatique.

Contenu du cours Sécurité Informatique pour Non-Informaticien

Principes généraux de la sécurité informatique

Domaines concernés : intégrité, disponibilité, confidentialité, authentification, imputation, traçabilité...
Notions fondamentales : authentification simple et forte, système de confirmation 3D, défense en profondeur, PRA/PCA ...
Démarche générale à entreprendre / analyse des risques

Les différents types de vulnérabilités et types d'attaques

Attaques : terminal, réseaux, applications (sniffing, DCI/DCI, DDoS ...)
Malwares : cheval de Troie, Virus, Rootkit, Spyware...
Attaques de mots de passe, injection SQL, vol d'identité et de données
Évaluer les risques

Techniques de protection - Fonctionnement des équipements dédiés

Cryptage : triple DES / AES
Séparation des flux par la formation des réseaux virtuels (VLAN)
Cryptage des données en ligne (VPN SSL et VPN IPSec)
Authentification d'accès : 802.1x / EAP Networks Access Control (NAC) et Role Based Access Control (RBAC)

Filtrage : firewalls protocolaires, de contenus, d'applications, d'identité...

Filtrage des applications Web : WAF (Web Access Firewall)

SIEM (Security Information and Event Management)

IAM (Identity et Access Management)

DLP (Data Lost Prevention) - Data Masking – Cryptage

Empreintes logicielles et MAC (Mandatory Access Control)

Autres domaines spécifiques

Plateformes spécialisées dans la sécurité informatique

Plateforme de Cloud de Sécurité (SecaaS : Security as a Service)

Plateforme de sécurité NGFW (Next Generation of Firewall)

Plateforme de gestion et de sécurité des mobiles EMM (Entreprise Mobility Management)

Combiner les solutions pour renforcer la sécurité

Sur Internet (communication et transaction) : cryptologie PKI (Public Key Infrastructure) / standard des échanges bancaires PSI-DSS

Pour les réseaux sans-fil Wi-Fi : 802.11i (802.1X/EAP...) / WPA / WPA2

Terminaux et applications mobiles (ODE, conteneurisation, App Stores, empreintes logicielles, App Wrapping...) / Banalisation du terminal et publication d'application (TS-WEB, VDI...)

En cas de BYOD (équipements personnels utilisés dans le cadre professionnel)

Pour la protection du Big Data et dans le Cloud (encryptions, vol de données, flux de données...)

Mesurer les bénéfices des actions de sécurité

La performance globale du système informatique

L'architecture du système d'information

Les référentiels à suivre

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ENISA (organisme Européen - gestion des risques), NIST (standards suivis par des grands acteurs du secteur de sécurité)

CSA (Cloud Alliance Security) / CSA Big Data / CSA Mobile

CNIL (Obligation Légale de sécurité)

Critères communs