Formation Sécurité du Système d'Information pour non informaticien

Objectifs de la formation Sécurité du SI - Introduction

Cette formation Sécurité du système d'information s'adresse aux non informaticiens. Concrète et complète, elle constitue une introduction aux briques techniques fondamentales présentes dans toutes les infrastructures systèmes, réseaux et applicatives des Systèmes d'Information (SI).

Au cours ce cette formation, nous vous expliquerons le fonctionnement des différentes infrastructures des systèmes d'information, ainsi que les failles de sécurité auxquelles toute entreprise est exposée, quelle que soit sa taille. Vous découvrirez les leviers sur lesquels agir pour se protéger, puis comment le SI s'ouvre vers l'extérieur, techniquement et au niveau des applications. Vous comprendrez ainsi pourquoi la transformation digitale des entreprises (ouverture du SI aux clients, aux fournisseurs, etc.) couplée à la place grandissante du Cloud dans les architectures doit être accompagnée de mesures de sécurité spécifiques à chaque outil ou fonctionnalité -infrastructure, poste de travail, annuaire d'entreprise, téléphonie, messagerie, Office 365, G Suite, applications, toutes les variantes « as a service », etc. Plus que jamais, le fait de comprendre votre architecture IT et son évolution programmée, tout en disposant d'une vue claire et objective sur la sécurité, vous sera indispensable afin d'échanger avec les acteurs internes et externes du système d'information de votre entreprise.

À l'issue de cette formation, vous serez à même de :

- Comprendre le fonctionnement des infrastructures des systèmes d'information (SI)
- Savoir comment le SI s'ouvre vers l'extérieur, techniquement et au niveau des applications
- Comprendre la place du cloud et ses solutions pour l'entreprise

- Connaître les outils de sécurisation des systèmes d'information
- Connaître les différents types d'attaques informatiques et leur fonctionnement

À qui s'adresse cette formation ?

Public :

Ce cours pour non-informaticiens est destiné à toute personne qui désire comprendre en quoi consiste la sécurisation du système d'information de l'entreprise. Même sans connaissance IT particulière, les éléments techniques présentés dans cette formation, y compris dans la maquette, restent concrets et accessibles.

Prérequis :

Travailler quotidiennement sur un poste de travail en réseau (navigateur WEB, explorateur de fichiers, messagerie, etc.).

Contenu du cours Sécurité du SI - Introduction

Infrastructure système (OS), aspects essentiels à comprendre pour la sécurité

Comptes utilisateurs, groupes et droits sur les ressources
L'annuaire Active Directory de Microsoft
Intégration de postes informatiques dans l'annuaire
Stratégies de sécurité appliquées aux ordinateurs et utilisateurs de l'annuaire
Authentification LDAP et SSO
Travailler sous Linux au quotidien (shell, processus, navigation dans l'arborescence)
En quoi consiste la virtualisation d'un OS (système d'exploitation) ?
Qu'est-ce que cela change au niveau sécurité ?

Travaux Pratiques :

Mise en place d'un annuaire d'entreprise Active Directory (AD)
Création de groupes utilisateurs et mise en place de droits sur les dossiers partagés
Tests depuis des ordinateurs distants physiques et virtuels (VM)

Exemples de stratégies (GPO) de limitations d'accès aux ressources (applications, données) selon les profils

Connexion sur un serveur Linux, localisation d'un fichier, modification d'un paramètre du site web et redémarrage d'Apache

Le Cloud pour l'entreprise, aspects essentiels à comprendre pour la sécurité

Liens entre Cloud, Datacenter et Virtualisation

Intégrer tout ou partie de l'infrastructure d'entreprise dans le Cloud (cloud hybride)

Vocabulaire associé : IaaS, PaaS, SaaS

Les offres du marché : Azure, Amazon, G Suite, Apps, Office 365, etc.

Exemples de coûts associés aux exemples présentés

Est-on mieux protégé dans le Cloud ?

Travaux Pratiques :

Mise en place d'un serveur Microsoft dans le Cloud abritant un annuaire d'entreprise (AD)

Mise en place d'un serveur web sous Linux dans le Cloud (une simple page d'accueil)

Accès distants sécurisés aux serveurs précédents (RDP, Putty)

Utilisation de Office 365 avec des comptes crées en séance dans l'annuaire précédent puis utilisés par les participants

Partage des données autour d'un Google Drive

Mise en place de la sécurité dans l'annuaire AD sur le Cloud

Architecture et services réseau

Comprendre le réseau et son vocabulaire de base : adresse IP, masque, passerelle, routage

Différences entre adresses IP publiques et privées ?

Principes de fonctionnement d'une Box Internet, personnelle ou professionnelle

Comment reconnaître un équipement (PC, mobile, imprimante, etc.) physiquement sur le réseau ?

Automatiser la configuration IP des équipements (DHCP)

Comment résoudre les noms (www.site.fr) en adresse IP (DNS) ?

Comment relier le réseau Wifi et le réseau filaire (Point d'accès) ?

Les différents modes de sécurisation du Wifi

La place (physique) et le rôle du firewall dans le réseau
Gestion de la sécurité des équipements mobiles en entreprise (BYOD, MDM, etc.)
Comment les routeurs se « parlent » entre eux
Vue générale de l'acheminement d'un paquet de notre PC jusqu'à un site web
Un mot sur les adresses IPV6

Travaux Pratiques :

Présentation de la maquette d'un réseau d'entreprise inter-agences
Exemple de configuration réseau IP basique d'un PC accédant à Internet et/ou à une autre agence
Exemple de configuration basique d'un serveur DHCP en entreprise
Exemple de configuration réseau d'un équipement mobile accédant à Internet
Présentation d'un serveur DNS et de son paramétrage de base chez un hébergeur, pour comprendre les différentes résolutions effectuées par un DNS relatives comme les noms de domaine www.site.fr ou les mails

Sécurisation du réseau

Les éléments de filtrage de base (@IP, n°port, @Mac)
Philosophie d'un firewall (règles)
Philosophie et apport d'une DMZ
Éléments de cryptographie
Principes de fonctionnement d'un VPN (Virtual Private Network)
Architecture et apports des certificats
Architecture et apports d'un serveur d'authentification (RADIUS)

Travaux Pratiques :

Exemples de règles de sécurité simples sur un firewall en production
Installation d'un certificat de type bancaire sur un PC
Exemple commenté de maquette d'une architecture d'entreprise avec accès distant sécurisé (VPN)

Fonctionnement des sites / applications web, aspects essentiels à comprendre pour la sécurité

Le vocabulaire du développeur (source, exécutable, interpréteur, runtime, scripts, bibliothèque, module, etc.)
Les modes de fonctionnement des applications (connecté / déconnecté, synchrone / asynchrone)
Comment une application « utilise » le réseau ?
Les grandes lignes du protocole TCP
Identifier les applications par des numéros (port)
Exemples parmi les standards (web, messagerie, bureau à distance, etc.)
Pourquoi d'autres protocoles (UDP, RTCP, etc.) ?
L'omniprésence du XML/JSON dans les échanges
Le langage de base du web (HTML)
Un mot sur la place du JavaScript et des CSS dans une application web
Les échanges entre un navigateur et un site / application web (http)
Vue générale des SGBDR et du langage SQL
Principes d'un site web dynamique avec accès à une base de données

Travaux Pratiques :

Comprendre le dialogue avec une application distante depuis un navigateur ou un client lourd à travers l'observation des sessions en cours depuis le PC de chaque participant
Exemples de requêtes SQL sur une base MySQL
Analyse détaillée du téléchargement d'une page web accédant à une base MySQL depuis la saisie de httpp://www.site.fr/page.php jusqu'à l'affichage des données par le navigateur (il s'agit donc de comprendre les différentes phases traversées, les technologies sous-jacentes et dans le prolongement logique des explications les failles de sécurité potentielles associées)

Sécurisation des sites / applications web

Ouvrir les applications vers l'extérieur : clients, fournisseurs, public…
Principe général de fonctionnement d'un Web Service (API REST)
Différences techniques entre une liaison https et http
La protection de base des SGBD et des sites web (utilisateurs et droits)

La protection « réseau » des applications

Comment ouvrir son site web à la monétisation

Rôle du firewall dans l'architecture applicative de l'entreprise

Travaux Pratiques :

Comprendre le dialogue avec une application distante depuis un navigateur ou un client lourd à travers l'observation des sessions en cours

Exemple d'attaque par injection SQL dans un formulaire web

Exemple de règles de firewall relatives aux applications

Les attaques informatiques

La faille humaine (ingénierie sociale)

Typologie des différents mails malveillants

Comprendre le fonctionnement des Virus, Antivirus, Malwares, Ransomwares

Protection par défaut de Windows : où en est-on ?

Charte du « bon » comportements à adopter

L'espionnage de trames réseaux (sniffing)

Saturer un service volontairement (Déni de Service)

Piratage de session (Hijacking)

Hacking de serveur web

Le ciblage des équipements mobiles

Apports d'un MDM (Mobile Device Management)

Risques avec les objets connectés (IoT)

Les attaques non détectées

Travaux Pratiques :

Exemples de journaux avec traces d'attaques sur un firewall

Exemple de prise en main d'un serveur web sous Linux sans le mot de passe associé si certaines conditions ne sont pas respectées

Panel de mails malveillants et « dégâts » associés (réalisés sur des machines virtuelles isolées donc sans risque de propagation)

Observation de serveurs en production exposés sur le web (applications disponibles et

vulnérabilités)

Simulation de saturation d’un serveur web

Travaux Pratiques

Le formateur s'appuie sur une maquette représentant l’architecture d’une entreprise composée de plusieurs agences communiquant entre elles et accédant à Internet (sites web, Cloud, etc.). Cette maquette permet d'illustrer progressivement les applications incontournables (partage de fichiers, sites web, messagerie...), les bases de données accédées à distance par des applications et des sites web, les connexions distantes sécurisées sur les postes de travail des utilisateurs et les serveurs à travers différents modes de sécurisation (RDP, VPN, ssh, certificats, etc.), ainsi qu'une architecture réseau intégrant le Wi-Fi et les équipements mobiles. Une importance toute particulière est accordée au paramétrage de la sécurité des différents composants (poste de travail, serveur, base de données, site web...) avec un zoom sur les règles standards des firewalls de l’entreprise.