Formation ACE MULTIPASS
PKI : Mise en Œuvre (4 jours)

Objectif de la formation

La PKI a rendu le chiffrement, la signature et l'authentification transparentes pour les utilisateurs. Elle permet la gestion et la protection de certificats numériques. L'objectif de cette formation est d'aider le stagiaire à monter en compétences sur les activités suivantes liées à la PKI :

- Installer, opérer une PKI
- Délivrer, renouveler, révoquer des certificats
- Contribuer à un projet de mise en place de PKI
- Rédiger la documentation
- Être au fait des aspect légaux liés à la signature électronique
- Configurer des applications pour utiliser la PKI

Prérequis et profil des participants

Cette formation étant technique, les participants doivent avoir de bonnes connaissances en sécurité informatique, serveur Windows (Active Directory, Windows Server…), administration, protocoles Internet. Les publics visés sont les chefs de projets, ingénieurs, équipes de support, consultants cybersécurité, administrateurs

Programme

Introduction

- Les faiblesses des solutions traditionnelles.
- Pourquoi la messagerie électronique n'est-elle pas sécurisée ?
- Peut-on faire confiance à une authentification basée sur un mot de passe ?
- Les facteurs d'authentification
- Usurpation d'identité de l'expéditeur d'un message.
- SSH et Man in the Middle.
- SSH, l'usage du chiffrement asymétrique sans certificat.

Cryptographie

- Concepts et vocabulaire.
- Algorithmes de chiffrement symétrique et asymétrique.
- Fonctions de hachage : principe et utilité.
- Les techniques d'échange de clés.

La confiance numérique

- Présentation du standard X509 et X509v3.
- La délégation de confiance
- Signature électronique et authentification
- Certificats personnels et clés privées
- Exportation et importation de certificats

La documentation d'une PKI

- La politique de certification (PC)
- La déclaration des pratiques de certification (DPC)
- Les conditions générales d'utilisation (CGU)

L'architecture PKI

- Autorités de certification racine et intermédiaire
- Autorité d'enregistrement (RA).
- Modèles de confiance hiérarchique et distribuée.
- L'annuaire LDAP
- Génération de certificats utilisateurs et serveurs.

Conduite des projets PKI

- Les différentes étapes d'un projet PKI
- Choix des technologies
- La planification
- Le setup, paramétrage
- L'audit

La législation

- Les directives Européennes
- Valeur légale des signatures
- Les différents types de signatures
- La législation en France
- Le schéma de certification
- Articulation entre le RGS et eIDAS

Panorama des offres du marché

- L'approche Microsoft.
- Les offres commerciales dédiées : Betrusted (ex-Baltimore) et Entrust.
- OpenPKI : la communauté Open Source.
- IdealX, entre solution commerciale et Open Source.
- Les offres externalisées Certplus, Versign...

Liste des ateliers et démos (à base de PKI Microsoft)

- Mise en œuvre d'une hiérarchie d'autorités de certification.
- Signature numérique de documents (PDF et office)
- Connection VPN à l'aide de certificat
- Authentication Web SSL v3
- Magasins de certificats Microsoft
- Mise en œuvre d'un serveur de messagerie sécurisé
- Inscription automatique des certificats utilisateurs (auto-enrollment)
- Inscription des utilisateurs avec agent d'inscription (enrollment agent)
- Mise en œuvre de répondeur OCSP
- Configuration et publication des listes de révocation des certificats (CRL)
- Linux : Mise en évidence lacunes protocolaires, installation et configuration d'un serveur SSH

En option (sur demande)

- L'architecture crypto de Windows (CSP, CAPI, CNG, KSP, base de registres etc)
- PKI et cartes à puces (gestion des lecteurs, cartes à puces etc)
- Le standard RSA PKCS11