Public Key Infrastructures («PKI»)

Savoir édifier l'architecture et les composantes d'une Public Key Infrastructure, connaître les solutions aux problèmes survenant lors de sa construction ainsi que les éléments auxquels il faut prendre garde en définissant le contenu des certificats.

Durée: 2 jours
Prix : 1'700.– excl. 8.1% TVA
Documents : Manuel de cours

Contenu

Dans les débuts d'Internet, personne ne se souciait des problèmes de sécurité. Aujourd'hui, les dangers d'une mise en réseau mondiale sont connus et tout le monde désire protéger ses informations électroniques.

Une infrastructure Public Key (PKI) est un outil efficace pour la protection des systèmes et des services sur Internet. PKI, bien qu'en développement depuis plus de 20 ans, n'est devenu un thème important pour les responsables de la sécurité que durant ces quelques dernières années.

Public Key Cryptographie est une technologie mûrie, qui forme la base des protocoles sécurisés. Pendant longtemps, il n'a pas existé de mécanisme strandard destiné à la distribution de Public Keys.Toutefois, des progrès ont été réalisés de nos jours concernant ces deux aspects. Il n'est pas nécessaire d'être un expert de Public Key Cryptographie pour en connaître ses avantages. Différents produits sont actuellement sur le marché. Ce cours aide à faire le bon choix parmi les nombreuses possibilités offertes et à en réaliser l'implémentation avec succès.

Contenu 1ère journée : Théorie

1. Introduction
    - Données du problème
    - Historique
    - Aspects juridiques
2. Bases de la cryptographie
    - Procédures symétriques et asymétriques
    - Signatures numériques
    - Key Management
3. Authentification
    - Base du mot de passe
    - Mots de passe à une seule utilisation
    - Cerberos
    - Certificats Public Key
4. Base PKI
    - Certificats
    - Certificate Revocation List
    - Policies
    - Voies de certification
5. Composantes PKI
    - Certification Authority (CA)
    - Registration Authority (RA)
    - Repository
    - Archivage
    - Propriétaire de certificat

    - Relying Party
6. Structure PKI
    - CA particulier
    - Infrastructure hiérarchique
    - Structure réseau
    - CertificationCross
    - Ponts CA
7. Vérification
    - Construction et contrôle des voies de certification
8. Certificate Revocation List (CRL)
    - Contenu
    - Production et distribution des CRLs
9. Directories
    - X.500, LDAP
10. Certificats X.509
    - Types ASN.1
    - Contenu de base
    - Extensions
    - Utilisation
11. Confidentialité, expirations, politique
    - Certificate Policies (CP)
    - Certificate Practice Statement
12. Applications
    - Web: SSL/TLS
    - E-Mail: S/MIME
    - IPsec

Contenu 2ème journée : Pratique

Construction d'un environnement de Certification Authority en deux étapes avec un Stand-alone Offline Root Certification Authority

- Construction d'un Enterprise (basé sur AD) Online Sub Certification Authority sous-jacent
- Qu'est ce qui est configuré différemment, lorsque seulement un environnement de CA (Enterprise Root CA) à un seul niveau est utilisé ?
- Utilisation des CaPolicy.inf Files
- Liste de configuration de verrouillage (CRL) complète et correcte, y compris la configuration d'Online Responders
- Configuration des modèles de certificats
- Configuration automatique de la demande, distribution et renouvellement de certificats par l'intermédiaire de GPOs
- Configuration correcte et installation de certificats SSL
- Révocation de certificats
- Configurations spéciales : archiver une clé privée, installer les agents de certification, etc.
- Surveillance des autorités de certification
- Sauvegarde et restauration des autorités de certification
- Utilisation des outils de ligne de commande (p.ex. certutil.exe) et PowerShell pour la configuration et la gestion des autorités de certification

Objectifs

- Présenter une structure et les composantes d'une infrastructure Public Key
- Connaître les solutions aux problèmes liés à l'édification d'une infrastructure Public Key
- Savoir à quoi vous devez prendre garde en définissant les contenus des certificats
- Connaître les réponses les plus importantes concernant les applications standards

Après le journée pratique, vous serez en mesure de mettre en place tous les éléments nécessaires d'un environnement PKI complet et le configurer, gérer, sécuriser ou effectuer du troubleshooting.

Méthodologie & Didactique

Ce cours est divisé en deux parties : le premier jour de cours est axé sur la théorie, le deuxième jour sur la mise en pratiques des connaissances acquises le premier jour.

Public cible

Développeurs et architectes techniques désirant élaborer une PKI ou créer des applications protégées.

Formations complémentaires

- Administering Microsoft Endpoint Configuration Manager («55348A»)

Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-securite/cybersecurite-defensive/cours-public-key-infrastructures