Gérer la sécurité des smartphones et des tablettes

Aujourd'hui, la quantité de terminaux mobiles dépasse celle des PC et le nombre de menace sur ces appareils croit de manière exponentielle. Or beaucoup d'utilisateurs professionnels considèrent leur appareil mobile comme un deuxième ordinateur. Ils consultent leurs messageries et veulent aussi un accès aux données métier. La sécurité mobile devient alors un enjeu stratégique pour les organisations.

Compétences visées

- Identifier les vulnérabilités des smartphones et des tablettes
- Gérer la sécurité par l'EMM (Enterprise Mobile Management)
- Mettre en place une veille de la sécurité mobile

Objectifs pédagogiques

- Identifier les vulnérabilités des appareils mobiles
- Lister les technologies et les solutions pour protéger les plates-formes et les applications mobiles
- Définir la sécurité des usages professionnels dans le cadre du BYOD (Bring Your Own Device)

Public

Responsable informatique, consultant, manager du SI, RSSI, DPO, chef de projet

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Introduction

- Définir les tendances actuelles
- Lister les impacts business

Identifier les vulnérabilités

- Lister les vulnérabilités des smartphones et tablettes
- Définir les risques d'escalade de privilège
- Lister les attaques des systèmes d'exploitation mobiles
- Expliquer les différents niveaux d'attaque

Gérer la sécurité par l'EMM (Enterprise Mobile Management)

- Définir le MDM (Mobile Device Management)
- Définir le MAM (Mobile Application Management)
- Définir le MCM (Mobile Content Management)

Mettre en œuvre un MDM

- Permettre une utilisation limitée à certaine zones géographiques
- Renforcer les couches logicielles et créer une Trust Zone
- Suivre les consommations
- Sécuriser l'accès de l'utilisateur au terminal

Mettre en œuvre un MAM

- Isoler par les containers
- Gérer les stores privés et autorisés
- Cloisonner les interactions entre terminal et serveur

Mettre en œuvre un MCM

- Sécuriser les mobiles contre les fuites des données
- Surveiller les activités
- Mettre en place le chiffrement des données
- Proposer un stockage sécurisé et partagé pour les mobiles

Gérer la sécurité des appareils personnels BYOD

- Insérer le terminal dans l'EMM
- Responsabiliser l'utilisateur
- Fixer un cadre légal d'utilisation

Gérer la sécurité de l'accès aux serveurs

- Lister les solutions : VPN SSL, Firewall
- Mettre en place une authentification forte d'accès aux réseaux
- Sécuriser pour la GSM/4G et le WiFi

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
13 et 14 septembre 2018
5 et 6 novembre 2018

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans la sécurité des appareils mobiles.

Après cette formation, vous pouvez suivre les formations RSSI, Les principes clés des normes ISO 27001 et ISO 27002, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.