Formation Sécurité des appareils et des applications mobiles

Objectifs de la formation sécurité mobile

D'ici 2020, Gartner estime que plus de 80% des accès utilisateurs aux applications d'entreprises se feront via les mobiles. Le mobile est un univers différent et les entreprises font donc face à un véritable challenge pour sécuriser les applications mobiles et les données éventuellement de grande valeur qui y sont associées. Le développement mobile reste assez neuf et les développeurs peuvent être tentés de se consacrer au fonctionnel et à l'ergonomie sans intégrer dès la conception la dimension sécurité.

Cette formation sur la sécurité des applications mobiles vise à vous présenter dans un premier temps le panorama des vulnérabilités et des solutions spécifiques aux plates-formes mobiles. Ensuite différents chapitres sur les logiciels de gestion de flotte mobile au niveau matériel (MDM, Mobile Device Management), applicatif (MAM, Mobile Application Management), et contenu (MCM, Mobile Content Management) vous permettront de disposer d'un échantillon très précis de solutions pour sécuriser votre flotte mobile.

Enfin, et c'est incontournable vu le thème de la formation, nous abordons les risques et solutions liés à l'utilisation d'un équipement personnel dans l'entreprise (BYOD). Parmi les thèmes clefs nous retrouverons les concepts de VPN, firewall, authentification réseaux, cohabitation Wifi/4G/5G, etc. avant de terminer sur les orientations de demain en matière de sécurité mobile. A la fin de cette formation vous serez capable d'auditer la sécurité d'une architecture mobile existante et de proposer des solutions.

À qui s'adresse cette formation ?

Public :

Toute personne concernée par un projet mobile.

Prérequis :

Bases en informatique et télécom (comprendre des termes comme serveur, firewall, Wifi, 5G, etc.).
Cette formation ne cherche pas mettre en œuvre la solution de tel ou tel éditeur mais à en dresser un inventaire objectif.

Contenu du cours sécurité mobile

Identification de vulnérabilités des plates-formes mobiles

Caractéristiques techniques et vulnérabilités des tablettes et Smartphones
Risques d'escalade de privilège (Jailbreak et Rooting)
Attaques d'Operating System (iOS, Android, Windows Phone)
Niveaux d'attaque d'une solution de mobilité : plate-forme terminale, applications, réseaux mobiles, donnée (contenu)

Panorama des fournisseurs majeurs de solutions de sécurité (MDM, MCM, MAM...)

Airwatch, Good Technology, MobileIron
Citrix XenMobile, IBM, Microsoft, SAP/Afiria
Vision et capacité opérationnelle des acteurs dans un marché en développement
Commercialisation : appliance-serveur privé et Cloud SaaS des solutions de sécurité

Sécurité par la gestion des appareils mobiles (MDM)

Description des caractéristiques communes des solutions MDM (Mobile Device Management) : prise en main à distance, géolocalisation des terminaux, vérification de conformité....
Utilisation limitée aux zones géographiques (exemple de solution)
Renforcement des couches logicielles (SE Android) et création de la Trust Zone (étanchéité)

Suivi de consommation

Accès de l'utilisateur au terminal

Métriques et critères essentiels de sélection des solutions

Sécurité par la gestion des applications (MAM)

Description des caractéristiques communes des solutions MAM (Mobile Application Management) : mise à jour automatique des applications, installation interdite des Apps....

Isolation par les containers

Apps Stores privés et autorisés : intégration des applications de l'écosystème par des API et connecteurs

Séparation des interactions entre les applications du terminal et du serveur

Métriques de qualité et critères principaux de choix

Sécurité par la gestion des contenus et données (MCM)

Définition du MCM (Mobile Content Management)

Sécurité contre les fuites des données (DLP)

Sécurité par la surveillance des activités (SIEM)

Encryptions gérées des données (On Device Encryption FIPS 140-2 (AES))

Cloud de stockage sécurisé et partagé pour les mobiles

Sécurité des terminaux mobiles personnels utilisés dans le cadre professionnel (BYOD)

Définition du concept BYOD (Bring Your Own Device)

Isolation par la virtualisation du terminal associée aux MDM et MAM

Sécurité par la responsabilisation : fixation d'un cadre légal d'utilisation (chartre d'utilisation, confidentialité CNIL...)

Sécurité de la connectivité des terminaux aux serveurs d'applications

Solutions existantes : VPN SSL, Firewall

Authentification d'accès aux réseaux : NAC et RBAC

Sécurité selon les types de réseaux GSM/4G/5G et WiFi et les lieux de connexion

Impacts et grandes tendances

Banalisation et abstraction des plates-formes terminales mobiles

Convergence des solutions mobiles et traditionnelles "fixes"

Refonte des dispositifs de sécurité actuels

Travaux Pratiques

De nombreux exemples concrets viennent ponctuer cette formation Sécurité Mobile afin de lié la pratique à la théorie.