Formation Sécuriser les réseaux VoIP

Description de la formation Sécurité Voix sur IP

La sécurité des réseaux VoIP est à l'heure actuelle le parent pauvre de ce type de technologie. Les nouvelles menaces qui pèsent sur ces architectures récentes sont de nouveaux défis pour tous les professionnels de la téléphonie qui n'était pas confrontés en voix classique à ce type de dangers

Objectifs

Ce stage très pratique et technique vous montrera comment sécuriser des réseaux Voix sur IP. À l'issue de cette formation, vous saurez vous prémunir efficacement contre les différents risques encourus, les participants sauront définir une stratégie de sécurité, sécuriser les réseaux de transport de la voix et maintenir un niveau de sécurité constant dans le temps.

À qui s'adresse cette formation ?

Prérequis :

Les participants doivent avoir de bonnes bases sur TCP/IP et des notions de Téléphonie et de Voix/IP

Contenu du cours Sécurité Voix sur IP

Introduction VOIP et sécurité

Définition et concepts
Problématiques de sécurité en générale.

Pourquoi sécuriser son réseau

De quoi doit on se protéger, de qui, pourquoi peut-on être attaqué ?

Les architectures VOIP

Les protocoles SIP et H323

Le protocole IAX, le protocole Open-source.

Les protocoles Annexes : MGCP, MEGACO, SIGTRAN, SIP-T

L'architecture d'opérateur.

IMS, IP Multimédia Subsystem : l'architecture des réseaux de demain.

La qualité de service et la performance.

Les menaces connues

La confidentialité : protéger les flux media et les données de type signalisation.

L'intégrité : contrôler et empêcher les modifications des données transmises sur le réseau

La disponibilité et le déni de service.

L'usurpation d'identité : les détournements rendus possibles grâce à la VoIP et les parades.

La fraude : surfacturation, détournement d'identité...

Le spam : les cas d'école. Comment détecter et lutter contre le phénomène.

La réglementation : les obligations légales de sécurité et les freins aux développements technologiques.

La sécurité des standards

H323

Les failles et les faiblesses du protocole

Les mécanismes de sécurité complémentaires de la suite de protocoles H323

H.235v2

H.235v3

H.323 Annexe J

SIP

Les failles et les faiblesses du protocole

Les mécanismes de sécurité proposés par les RFC SIP

Authentification des flux de signalisation par les mécanismes de type HTTP Digest

Utilisation de S/MIME pour la sécurisation des flux de signalisation

Confidentialité des flux média

Utilisation de TLS avec SIP

Intégration d'IPsec et SIP

Les améliorations futures de SIP en matière de sécurité

Les problématiques de sécurité des protocoles d'opérateurs

Forces et faiblesses de MGCP

Forces et faiblesses de Megaco

Firewalls et NAT

Les Firewalls

Le rôle du firewall

Statefull/Stateless

Les spécificités de la VOIP : la problématique des ports dynamiques, les protocoles parapluie...

La translation d'adresse (NAT)

Le problème de l'adressage IP : adressage privé, adressage public, évolution IPv6...

Les solutions et les architectures actuelles : les technologies STUN, TURN, ICE, UPnP.

NAT et Firewall : les impacts sur la QoS

Les compromis Qualité de Service vs Sécurité.

Les impacts sur les mécanismes d'établissement d'appels

Les effets sur la qualité de service : les flux média

Les solutions envisagées

Les ALG : Application Level Gateways, l'intelligence VoIP intégrée aux firewalls.

Les boîtiers intermédiaires : des serveurs dédiés VoIP de contrôle dynamique de la sécurité.

Les SBC : Session Border Controllers. Les solutions intégrées de sécurité.

Les VPN.

Les VPN et le cryptage

Le rôle des VPNs.

VoIPsec

L'association IPSec et VoIP

Les difficultés d'implémentations

TLS : Transport Level Security

Principes : Sécuriser les flux de signalisation

Intégrer TLS avec les protocoles VoIP.

Les impacts sur la qualité de service

Le moteur de cryptage

La taille des paquets

SRTP : Secure Real Time Protocol

Principes : Sécuriser les flux de média

Le protocole de gestion des clés des environnements multimédia : MIKEY.

Convergence VoIP

Les environnements

Le LAN

Le WiFi

Le Bluetooth

Le WAN

Les protocoles secondaires

TFTP

DNS

DHCP

Travaux Pratiques

De nombreux travaux pratiques permettront aux participants de manière à mettre en pratique les notions présentées. Des études de cas seront également présentées à partir d'architecture d'entreprise, d'architecture d'opérateur et de Skype