NIMBUS TRAINING
La formation NTIC • Tél : 02-40-85-19-32• cedric.tron@nimbus-training.fr

Sécurisation des serveurs internet et intranet – Mise en oeuvre

Déscription :

Avec Internet, les réseaux sont dorénavant ouverts et par conséquent, beaucoup plus exposés aux attaques virales ou autres actes de piratage. Il est donc devenu primordial de savoir faire face à ces différents risques pour protéger les données de l'entreprise et garantir l'intégrité et le bon fonctionnement de son système d'information

Objectifs

- Évaluer les risques internes et externes liés à l'utilisation d'Internet
- Comprendre comment garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes
- Acquérir une méthodologie pour la mise en œuvre de la sécurité des réseaux

Publics

Administrateurs et techniciens systèmes et réseaux, responsable sécurité

Durée

4 jours

Pré-requis

Bonnes connaissances sytèmes Windows et Unix ainsi que des protocoles TCP/IP

Programme de cette formation

Développer la politique de sécurité

- La sécurité et la continuité
- Les applications et les outils disponibles

La sécurité des systèmes Unix et Windows

- La gestion de l'authentification (Radius, Kerberos)
- La gestion de services réseau

La sécurité client

- Les certificats clients
- Les options de sécurité des navigateurs

La sécurité serveur

- L'authentification des utilisateurs
- Protéger l'accès au serveur

Mise en place de l'Intranet via le réseau public

- Le déploiement d'un réseau privé virtuel (VPN)
- Les méthodes d'authentification (PAP, CHAP)

Les méthodes de piratage et les types d'attaques

- Les attaques sur les protocoles
- Les faiblesses des services
- Les virus et chevaux de Troie

La mise en place de certificats

- Les serveurs de certificats
- Les certificats numériques

Les techniques cryptographiques

- L'objectif du cryptage
- Les normes et leurs possibilités

Les serveurs proxy

- L'architecture d'un proxy
- La gestion des proxies avec des firewalls

Architecture et configuration des firewalls

- Les différents types de firewalls
- Les règles du filtrage
- Les règles et de la translation d'adrsse
- La mise en oeuvre d'une DMZ
- L'intégration d'un firewall dans le réseau d'entreprise

Détection et surveillance des faiblesses

- Les informations à surveiller
- Analyse du trafic réseau

Mise en place de la sécurité des données de l'entreprise

- Évaluation des besoins de l'entreprise
- Règles de la mise en place d'un plan de sécurité
- La veille technologique
- Les organismes officiels
- Les coûts