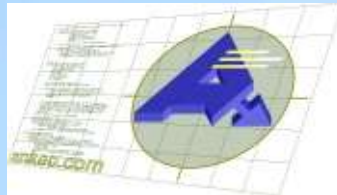


Sécurité et mobilité

Jean-Marc Boursot



<http://www.ankeo.com>

© Ankeo 2003 - reproduction interdite

Ankeo

- Société de conseil spécialisée en sécurité informatique et réseau
- Audit, conseil en sécurité
- Firewalls, tests de vulnérabilités, veille technologique, etc.
- Conseil, ingénierie en logiciel libre

Buts de la sécurité

La sécurité 100% n'existe pas mais on cherche à améliorer:

- disponibilité du système
- intégrité des données
- confidentialité des échanges
- identification des acteurs

Principes

« *La sécurité n'est pas un produit mais un processus...* »
(Bruce Schneier - *Counterpane Security*)

4 axes de travail :

- **prévention**

politique de sécurité, formation, sensibilisation des utilisateurs, sauvegarde, etc.

- **protection**

firewall, antivirus, chiffrement, authentification, etc.

- **détection (et évaluations)**

surveillance et journaux, audit, veille technologique, systèmes de détection d'intrusion, etc.

- **correction (et réponses)**

mise à jour des logiciels, changements des paramètres, adaptation de l'organisation, restaurations, etc.

Problèmes de la mobilité

- Matériels hétérogènes et évoluant dans un environnement non contrôlé
- Moyens de connexion hétérogènes
- Authentification matérielle et souvent pas d'authentification individuelle
- Transport d'informations hors de l'entreprise
- Intégration au système d'information et dans la sécurité existante (firewall, sauvegarde, ...)
- Pistage de l'itinérant

Solutions

- Politique de sécurité stricte
- Chiffrement des communications: réseau privé virtuel (VPN), web sécurisé, etc.
- Cloisonnement des réseaux (authentifier les équipements puis les individus)
- Chiffrement des données stockées
- Sauvegardes

Le cas du Wifi

- **Avantages**

- mise en oeuvre facile, rapide et peu coûteuse
- réseau flexible et adaptable
- mobilité

- **Inconvénients**

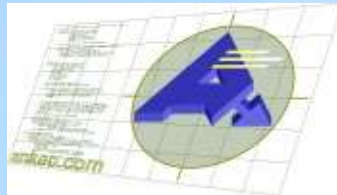
- réseau ouvert ne s'arrêtant pas aux portes de l'entreprise (détection, intrusion, écoute illégale, brouillage, usurpation de point d'accès)
- accès anonyme
- système de chiffrement WEP faible

- **Sécurité**

- considérer la partie « sans fil » comme un réseau externe hostile
- gérer la sécurité physique des ondes dans l'espace
- introduire des authentifications et chiffrements forts

Sécurité et mobilité

Jean-Marc Boursot



<http://www.ankeo.com>

© Ankeo 2003 - reproduction interdite