

Guardis

Les Solutions VPN : Aspects Sécurité

Février 2005

Introduction

- Définir ses **besoins REELS**
- Déterminer les **risques REELS** liés
 - à ces besoins
 - à son environnement
- Choisir les outils **adaptés**
 - qui répondent aux **besoins ET aux risques**
 - en assurant le **suivi** régulier

Définir ses besoins réels (évident ?)

- Quelles ressources ?
- ... pour qui ?
- ... à partir de quel(s) endroit(s) ?
- ... à quel moment ?
- Comment seront-elles accessibles ?
- ... et à quel prix (**budget**) ?

Déterminer les risques

- Sous l'oeil **global** de votre entreprise
 - Objectif : déterminer ses **points faibles**
 - Classement par **ordre** d'importance et liens
 - conséquences directes et indirectes ?
 - probabilité d'avoir lieu
- Exemples :
 - Commercial quittant l'entreprise (avec des dossiers ?)
 - Gros client qui « tarde » à payer ...
 - Vol ou panne du matériel
 - Collaborateur absent (informaticien ?)

Déterminer les risques

- Sous l'oeil de vos **infrastructures informatiques**
 - Objectif : déterminer ses **points faibles**
 - Classement par **ordre** d'importance et liens
 - conséquences directes et indirectes ?
 - probabilité d'avoir lieu
- Exemples :
 - Confiance en ses collaborateurs
 - Vol ou panne physique d'un serveur / PC / router / Firewall
 - Virus / intrusion / abus de ressources
 - Perte de données

La problématique du VPN

- Le VPN
 - c'est **partager** ses ressources
 - donc **augmenter le risque** global de l'entreprise

Les risques **spécifiques** aux VPNs

L'impact sur les **autres risques** de l'entreprise

Les risques spécifiques des VPN

- Vol / perte d'un portable avec les clés d'accès
- Virus / intrusion sur un portable ou un site distant
- Mauvais droits d'accès / gestion des utilisateurs
- Erreur de (re)configuration / erreurs humaines
- Risque de cascades
- Risques technologiques

Les aspects sécuritaires des VPN

- **La confidentialité**
- **L'intégrité**
- **Le contrôle de l'identité / authentification**
- **La disponibilité**
- **L'intégration et l'évolution**

Les aspects sécuritaires des VPN

- **La confidentialité**
 - Méthode de cryptage
 - Niveau de cryptage
- **La disponibilité**
 - dans les temps / aux bonnes personnes
 - vitesse / redondance
- **L'intégration et l'évolution**
 - avec le reste de l'infrastructure (Firewall – AntiVirus - ...)

Les aspects sécuritaires des VPN

- **Le contrôle de l'identité / authentification**
 - du simple mot de passe ...
 - ... au système PKI complet
 - en passant par les méthodes bio-métriques
- **L'intégrité**
 - Garantir la non corruption lors des transferts
 - des données
 - des mécanismes d'authentification

Les technologies

- Méthodes sécurisées
 - VPN IPSec
 - SSL
 - autres méthodes
- IPVPN et MPLS, BiLan et autres technologies d'ISP
- Lignes propriétaires / Wi-Fi

Le choix des technologies

- **En fonction du risque**
- **Mais aussi de la facilité**
 - d'installation
 - d'intégration
 - d'utilisation
 - de maintenance
 - d'évoluer / adaptation (technique ou autre)
- **Et bien sûr des coûts (directs et indirects)**