

# ● Sécurité des Réseaux



## NOS METIERS | ○

- Audit / Conseil  
Maîtrise d'œuvre  
Ingénierie
- Déploiement / Intégration  
Installation et paramétrage  
Formation et prise en main
- **Cabling**  
**Interconnexions de sites**  
**Solutions clients légers**  
**Sécurité**
- Solutions applicatives  
Web technologie  
ERP / Solution de gestion
- Centre d'Appel  
Assistance technique  
Services Après vente
- Externalisation  
Financement  
Infogérance

## La Sécurité, un enjeu économique et stratégique

Les systèmes informatiques contiennent des informations importantes du point de vue économique, politique et stratégique pour les entreprises et leurs collaborateurs. La sécurité doit être abordée dès la conception des systèmes d'information.

La sécurité doit être gérée à tous les niveaux, des éléments du réseau intranet (et son lien vers Internet) jusqu'à la gestion des comptes d'accès par les terminaux utilisateurs, afin de bloquer toute attaque du type intrusion, interception de données, virus, chevaux de Troie ou Spam.



## Notre Approche :

Faire une analyse détaillée spécifique, et ne pas penser produit dès le départ. Mettre en place les procédures internes complémentaires pour maîtriser les risques.

## Les trois questions test de COM6

Vos applications sont-elles protégées en accès externe depuis Internet?  
Avez-vous une gestion centralisée de vos mots de passe ?  
Tous vos postes de travail sont-ils équipés d'un anti-virus ?

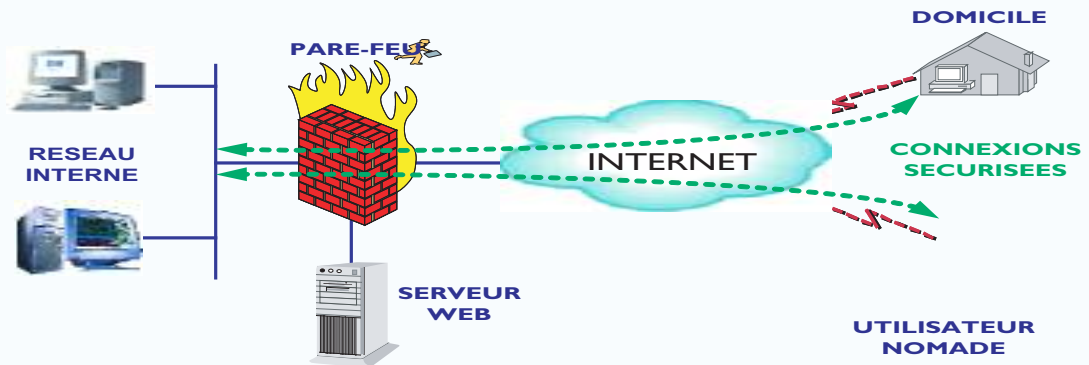
## Nos Partenaires :



### Base de réflexion :

- 75% des risques proviennent de l'intérieur de l'entreprise et non de l'extérieur (le personnel involontairement, les employés licenciés ou malveillants,...)
- Beaucoup d'entreprises ne tiennent pas compte des événements survenus sur leurs réseaux...
- Les SPAM et les tentatives d'intrusion peuvent occuper 100% de votre bande passante.

### **EXEMPLE D'ARCHITECTURE SECURISEE**



### Piliers de la sécurité:

- 1) **Les Logiciels Antivirus** : les virus doivent être détectés avant infection du PC utilisateur
- 2) **Les Pare-Feux** : équipement servant de barrière de filtrage entre différents réseaux (internes ou externes)
- 3) **Les Contrôles d'Accès** : authentification des utilisateurs (profils et droits d'accès)
- 4) **Le Cryptage** : permet de s'assurer que seul le destinataire autorisé pourra lire les données lui étant destinées. Evite l'interception de données.
- 5) **La Détection d'Intrusion** : système permettant de détecter des trafics non autorisés ou suspects en différents points d'un réseau
- 6) **L'Exploration du réseau** : détection des applications réseau non utiles afin de les supprimer, et détection des failles des différents équipements du réseau afin d'y remédier par le correctif associé
- 7) **L'Expertise** : évaluation de la politique de sécurité mise en place ainsi que des équipements utilisés et configurés. Est en général assurée par un expert sécurité.

### Notre méthode :

**A**uditer vos besoins, vos outils actuels et les vulnérabilités existantes.

**D**éfinir, mettre en œuvre et tester la solution.

**F**ormer votre personnel et assurer un support technique.

**A**ssurer une assistance pour réagir très rapidement à de nouveaux risques.

Pour en savoir plus sur les solutions Com6, contactez-nous au 0 825 000 136