

Compte-rendu

La question taraude celles et ceux dont l'activité professionnelle implique l'accès à distance à leur réseau d'entreprise : « Parmi les solutions d'accès à distance, quelle est la mieux adaptée à mon entreprise ? Quels dispositifs sécuritaires dois-je mettre en place ? »

Ce 22 février 2005, le **FORUM TELECOM** de la SPI+ a tenté d'y répondre en proposant à la cinquantaine d'inscrits d'écouter 3 experts en la matière ; Messieurs Olivier Roomans (Alteryx), Daniel Bartz (Guardis) et Eric Preud'homme (Computerland SLM).

Olivier Roomans, responsable Systèmes et Réseaux au sein d'Alteryx a brossé une vue d'ensemble des solutions d'accès distant existantes.

Il a présenté le **FTP** (File Transfer Protocol). Un protocole de transfert de fichiers utilisé sur Internet basé sur TCP-IP qui est limité au transfert de fichiers et qui ne permet pas de consultation en temps réel. Ce moyen simple de se connecter au réseau peut poser problème d'implémentation en cas de présence de firewall ou de partage de connexion.

Autre solution assez répandue ; le **Webmail**. Un moyen simple d'accéder uniquement à sa messagerie électronique à partir de n'importe quel endroit connecté à Internet en utilisant un simple navigateur Web.

Avec les **serveurs d'applications**, les programmes sont installés sur le serveur de l'entreprise et les workstations n'ont en charge que l'affichage des informations, la gestion des claviers et souris. La maintenance est limitée : tout n'est installé qu'une fois sur le serveur.

Les **applications légères**, programmées sur mesure sur le modèle client/serveur, existent sous différentes formes de technologies mais sont coûteuses. Toute l'intelligence se trouve du côté du serveur et on accède via un simple navigateur web.

Avec les **connexions asynchrones**, il s'agit de se connecter ponctuellement au réseau de son entreprise pour se synchroniser via son PDA par exemple.

Et la **connexion asynchrone avec stockage des fichiers sur un serveur intermédiaire indépendant** est un produit presque similaire. Mais les données étant stockées hors de l'entreprise, les aspects fiabilité et confiance en l'intermédiaire sont à prendre en compte.

Enfin, le **VPN** consiste en une solution permettant d'interconnecter des sites distants entre eux et/ou des télétravailleurs de manière sécurisée. En effet, il propose un tunnel cryptant les données. Ce codage et décodage des données ralentissent légèrement leur circulation. D'où l'importance d'une connexion Internet fiable afin que l'utilisateur voit le réseau de son entreprise comme si il y était connecté en local. La configuration des clients et serveurs est plus complexe car il faut générer des certificats pour chaque client ainsi qu'un mot de passe - deux mesures renforçant la sécurisation.

Et le VPN peut-être complémentaire aux techniques présentées plus haut.

Le deuxième orateur, Daniel Bartz, Managing Director de Guardis s'est attardé sur les aspects sécuritaires du VPN, attirant l'attention sur l'importance de **définir le plus précisément possible ses besoins réels** pour être sûr d'implémenter la technologie VPN adaptée. Pour faire ce bilan, des questions clés : « Quelles données voulez-vous partager, avec qui, à partir de quel(s) endroit(s), quand, via quel matériel (PDA, Smartphone, ordinateur portable,...), et à quel prix ? »

Il faut également **connaître les faiblesses de l'entreprise et de ses infrastructures informatiques** afin de déterminer les risques associés aux besoins. (Quelle confiance accordez-vous à vos collaborateurs, vos clients, votre anti-virus,... ?).

Car **l'implémentation d'un VPN augmente les risques** de vulnérabilité du réseau puisque plus de personnes vont avoir accès à plus de données dans plus d'endroits.

Techniques d'accès à distance au réseau d'entreprise (Virtual Private Network)

Une fois l'évaluation faite, il s'agit d'implémenter la formule idéale intégrant le respect de la **confidentialité** via le cryptage et la mise en place de ces algorithmes, le contrôle de l'**identité de l'utilisateur**, la certitude de **disponibilité d'accès**, de l'**intégrité** des données transférées et l'**intégration correcte du système** au reste de l'infrastructure existante (firewall, antivirus,...). Monsieur Bartz a insisté sur l'importance de garder les outils à jour et de pouvoir le faire facilement. **La sécurité est un processus permanent.**

Le troisième intervenant, Eric Preud'homme, Project Manager chez Computerland SLM a détaillé **3 exemples représentatifs** de solutions VPN.

En préambule, il a recommandé de ne pas choisir les technologies « d'avant-garde » mais de se fier aux systèmes qui ont déjà fait leurs preuves. Il s'agit d'éviter notamment les problèmes de maintenance

- Le **VPN IPSec**, adapté aux PME disposant de 2 ou 3 sites interconnectés et de commerciaux se connectant à distance via la technologie VPN IPSec. Cette solution convient pour l'échange de fichiers, la messagerie, application ERP.
- Le **VPN SSL**, une solution principalement utilisée pour les télétravailleurs mobiles (application Intranet, messagerie, échange de fichiers). Ici le protocole SSL assure une connexion sécurisée vers un boîtier intermédiaire qui établit la connexion vers l'entreprise.
- Et le système basé sur les **Serveurs d'applications** qui convient pour toutes les applications et qui est compatible avec tous les types de postes. Les données tournent dans le site central et rien n'est installé sur les postes distants. Seuls sortent les affichages. Il requiert une très faible bande passante puisque l'on ne reçoit que l'affichage des données.

Ces 3 exemples et leur coût estimé sont détaillés dans les slides de l'orateur.

En guise de conclusion, qui a fait l'unanimité chez les trois orateurs du séminaire, Monsieur Preud'homme a rappelé que **la sécurité de la solution implémentée est importante; elle ne s'achète et ne s'installe pas une fois pour toutes**. Il faut régulièrement faire vérifier les accès et les risques d'intrusions.

*Compte-rendu réalisé par Mme Claire GILISSEN pour le compte du **FORUM TELECOM**, initiative de la SPI+ bénéficiant de l'aide financière de la Région wallonne et du FEDER.*

<http://www.forumtelecom.org>