CHAPITRE 2 :

PRESENTATION DU THEME

1. Contexte

Dans le souci d'atteindre une sécurité sans faille, MTN CI par le biais de sa direction informatique nous demande à travers ce thème : « déploiement d'une solution de contrôle d'accès au réseau LAN pour les utilisateurs et invités : cas de MTN CI » d'établir une étude afin de permettre :

- Une bonne gestion de l'accès au parc informatique et au données de l'entreprise
- Une bonne administration du système de contrôle d'accès au réseau
- Une flexibilité de l'accès au réseau

2. Motivation de thème

L'objectif principal du contrôle d'accès étant de pouvoir limiter les allées et venues dans l'entreprise, il est primordial d'évaluer de manière précise les points à contrôler :

- Installation d'un système de contrôle d'accès au réseau adaptés aux besoins de l'entreprise
- Les équipements de contrôle d'accès multi-sites sont gérables à distance via une simple interface web *ou un logiciel installé en mode client / serveur*
- Assurer l'authentification des connexions
- Respecter les Règles de sécurité pour l'authentification des connexions : A savoir

  - Tous les utilisateurs de l'entreprise sont connus et associés à une matrice de droits d'accès aux ressources de l'entreprise.
  - Tous les accès au réseau d'entreprise (intranet) sont authentifiés. Cela concerne les accès des utilisateurs au réseau interne de l'entreprise aussi bien qu'aux ressources informatiques.
  - Les accès distants au réseau d'entreprise doivent être fortement authentifiés.
  - Les connexions de tierces parties ou de fournisseurs du réseau d'entreprise (extranet) sont authentifiées.
  - Aucune connexion directe au réseau interne de l'entreprise ne doit être autorisée.

3. Analyse et critiques

L'interconnexion des différents équipements en vue de fournir des services à créer des problèmes liés à l'évolution des technologies mises en interaction. Cependant même si elles ont été conçu pour faciliter les échanges de données, il faut souligner qu'elles donnent naissance à une nouvelle forme de menace qu'il faut contrer a tout pris. Nous pouvons citer parmi tant d'autres :

- Aucun contrôle d'accès : il n'y a pas d'authentification et n'importe qui peut se connecter au réseau soit par câble soit par wifi, sans qu'aucune authentification ne soit requise, même pas une clé de sécurité pour le point d'accès
- Aucune surveillance des activités sur le réseau : une fois connecté au réseau, l'on est libre d'aller et venir dans n'importe quelle machine sans restriction.
- Les postes de travail du personnel administratif sont accessibles par tous. Un utilisateur quelconque peut avoir accès aux informations de l'entreprise
- Une répartition anormale de la ressource internet : en effet, comme cela était le cas très souvent, internet était très sollicité par les stagiaires et consultant. Ceux-ci s'adonnaient à des téléchargements à longueur de journée, ce qui abaissait le débit au niveau des machines administratives. Cela se faisait ressentir lors de l'ouverture des pages web.

Ainsi donc La protection d'un réseau au sens de la défense contre les intrusions nécessite une réflexion adéquate pour la mise en œuvre des solutions. Il faudra veiller à paramétrer correctement chaque élément du réseau (ordinateurs, serveurs) afin qu'aucun d'entre eux ne soit une faiblesse dans la muraille en mettant un focus sur l'aspect humain.

A MTN CI la gestion de ce risque à occasionner une réflexion poussée qui à orienter les débats sur un moyen efficient de gérer l'accès à l'infrastructure.

4. Problématique

Le risque d'accès non autorisé lié au manque d'outils de contrôle définit la raison fondamentale de ce système. Le contrôle d'accès au réseau de l'entreprise représente un point essentiel pour son bon fonctionnement et sa capacité à subvenir au intrusions physiques sur le réseau. Dans notre cas, le manque de stratégie et d'outil de contrôle nous pousse à la recherche active d'une solution de contrôle d'accès au réseau.