1 Situation de départ et but

Hypothèse

Les employés de l'entreprise TELECOM SA n'avaient, jusqu'à présent, pas d'accès au réseau de l'entreprise par la connexion sans fil (Wifi). Un projet consiste à proposer cet accès à ses 160 personnes.

En tant qu'entreprise de télécommunication progressiste et orientée vers l'avenir, TELECOM SA cherche d'une part à familiariser le personnel avec les technologies nouvelles et d'autre part à faire appel à la responsabilité de chacun.

L'objet d'étude dans le cadre de cette analyse de risque est un segment du réseau LAN de taille moyenne situé dans un bâtiment administratif. Celui-ci est, comme tous les segments LAN de TELECOM SA, relié au réseau d'entreprise grâce à un routeur. Chaque segment compte environ 60 stations de travail. Certains segments connectent les serveurs.

Le segment LAN – faisant l'objet de cette analyse - dessert deux unités de TELECOM SA (le département « Voice » et « Mobile »). La responsabilité des serveurs et l'administration du réseau incombe au département « Voice ».

2 Données influentes

2.1 Conditions cadres

La connexion de tous les PC à Internet est effectuée au travers d'un firewall. Les sorties directes par modems/partage de connexion Internet via téléphonie mobile ne sont pas autorisées.

Les exigences de disponibilité du LAN doivent être considérées comme importantes. Nous admettons un temps d'interruption maximal de 2 heures (le cas échéant jusqu'au retour à une exploitation normale).

Dans le bâtiment administratif, le département « Voice » traite des données financières critiques et confidentielles.

Différents « Product Managers Voice » ont également leur place de travail dans ce bâtiment. Une activité importante des « Product Managers » consiste à acheter des produits destinés à la revente. Les appels d'offre et les offres sont élaborés sur les stations de travail de ces derniers. La comparaison des offres s'effectue au moyen de tableaux Excel. Le volume des offres peut devenir très important et la connaissance des offres concurrentes peut être très intéressante pour les soumissionnaires.

Le LAN dessert également une petite centrale d'impression située dans les sous-sols du bâtiment administratif. Cette centrale d'impression traite la plus grande partie des travaux du bâtiment (factures, décomptes, publications, etc.).

Les collaborateurs internes n'ont pas besoin d'avoir une autorisation spéciale pour accéder à Internet.

2.2 Architecture et topologie du réseau

2.2.1 Système d'exploitation

- MS Windows Serveur et Windows Workstation (Systèmes d'exploitation 64 bits).

2.2.2 Programmes standards

- Suite office (Office 365)
- Navigateur Internet (Chrome et Firefox)
- Antivirus (Symantec Norton).

2.2.3 Applications spécifiques

- SAP
- Suite graphique (Adobe)

2.2.4 Stockage des données

Les données ne sont en règle générale pas stockées au niveau des stations de travail (excepté pour les « Product Managers »), le stockage des données et leur traitement central sont effectués par les serveurs de données. Les responsables des stations de travail sont seuls compétents des données qui sont exceptionnellement et malgré tout traitées localement.

2.2.5 Télécommunication

Les laptops de TELECOM SA qui sont configurés en tant que stations de travail permettent le transfert de données. Ces laptops sont équipés de carte WiFi.

2.3 Exigences

2.3.1 Disponibilité

- Internet doit être utilisable 24 heures sur 24
- Le réseau interne ne doit pas être surchargé par l'utilisation d'Internet

2.3.2 Intégrité

- Les données et les programmes des serveurs internes ne doivent pas être menacés par un accès externe (Internet)
- Les stations de travail ne doivent pas pouvoir être manipulées depuis Internet
- Le réseau interne doit rester intègre

2.3.3 Confidentialité

- Les données et les programmes sensibles ne doivent pas être accessibles sans autorisation depuis l'extérieur (WAN)
- Les exigences liées à la protection des données personnelles doivent être remplies.

2.3.4 Collaborateurs

- Le personnel doit être instruit aux nouvelles technologies et sensibilisés aux risques inhérents
- La possibilité de télétravail au domicile de l'employé doit être offerte aux utilisateurs de laptops.

2.4 Risques et menaces

- Le risque « Internet » : Un seul PC du réseau interne insuffisamment sécurisé peut mettre en danger l'ensemble de TELECOM SA
- Risques liés aux protocoles : TCP (spoofing), UDP (diffusion de messages individuels), ICMP (révélation d'informations structurelles)
- Risques liés au trafic : Demande permanente de connexion (Mail-bombing), connexions laissées en suspens, connexions inutiles rejetées
- Risques liés à l'utilisation du WiFi : Ecoute active, usurpation d'identité, intrusion dans le réseau de production
- Usurpation : Utilisation d'un nom d'hôte ou de l'adresse IP d'une autre station de travail
- Virus, cheval de Troie, phishing (Attachements aux Courriels, download de software, ActiveX, Applets JAVA, etc.)
- Autres programmes destructeurs (« Ping of Death », etc.)
- Le risque humain : Méthode de travail peu soigneuse, manque d'information et de discipline (oubli de fermeture de sessions), non actualisation régulière des mots de passe, utilisation risquée d'Internet (partage de connexion) et des autres médias disponibles.
- Le risque de concurrence : Les concurrents montrent un grand intérêt pour certaines informations traitées sur le LAN.

3 Schéma de principe du réseau