

Étude de cas de la société Biz

1 – Recensement des menaces et des impacts

1 - En sécurité de l'information, nous parlons deux deux stratégies bien distinctes, la première est la sécurité logique qui protège les informations numériques stockées sur l'ordinateur. La deuxième est la sécurité physique qui elle protège le matériel. Commençons par celle-ci.

L'ordinateur portable crée de nouvelles menaces pour l'entreprise. En effet, contrairement à du matériel fixe stocké dans les locaux, il peut plus facilement être victime d'un vol ou d'une chute.

Les dirigeants et l'équipe informatique devront donc penser à cela au moment de l'achat pour se doter de machine particulière. Par exemple doté de disque SSD ou « d'airbag » pour disque dur qui protégeront les données du disque dur. Cela dans le cas où ils comptent que des données sensibles soit stockées sur l'ordinateur.

Pour le vol, ils devront prévoir des séances de sensibilisation destinée aux commerciaux et des assurances précises pour éviter les surprises.

Mais cela ne suffira pas. En effet, si l'ordinateur est volé, l'individu pourra avoir accès aux données stockées sur le PC. Il faudra donc que le personnel informatique équipe et paramètre les PC portables de logiciels de sécurité (cryptage des données, mot de passe fort, etc ...) pour éviter l'espionnage industriel qui pourrait être réalisé suite au vol. Mais il faudra aussi des logiciels s'occupant de la sauvegarde (ou synchronisation) des données pour ne pas, en plus, perdre des données. C'est ces points traitant de la protection des données qui caractérisent la sécurité logique.

2 - Cependant, le matériel mobile n'entraîne pas que ces menaces. Il devient aussi une menace pour le réseau interne de l'entreprise car des données transiteront entre ces PC portables et le matériel interne.

Pour cela, il faudra que les deux employés informatique pensent à deux types de menaces :

- Celles liées à la connexion des commerciaux de l'extérieur vers l'intérieur du réseau
- Et celles liées à la présence des commerciaux au sein de l'entreprise et qui seront directement reliés à l'interne du réseau

Pour la sécurité du réseau quand les commerciaux sont à l'extérieur, il faudra que l'entreprise se dote d'un serveur VPN qu'elle pourra isoler au sein d'une DMZ pour ne pas faire courir de risque au reste du réseau. En effet, l'usurpation d'adresse mac ou IP étant simple, il ne faudrait pas qu'une autre personne ou un autre portable puisse se connecter au réseau interne de l'entreprise depuis une connexion internet.

Le VPN permettra, donc, aux employés d'avoir un accès sécurisé de l'extérieur et grâce à cela ils pourront être considérés comme faisant partie du réseau local et donc auront le droit d'accéder aux ressources nécessaires.

Mais cela ne suffira pas, l'investissement dans un ou plusieurs firewall sera nécessaire pour que le réseau soit sécurisé de manière sur. Tout d'abord il sera plus efficace que le routeur filtrant et ensuite il permettra de créer les DMZ nécessaires en toute sécurité.

Il évitera, entre autre, à un pirate de rebondir ou bon lui semble dans le réseau interne, en cas d'attaque réussie.

Enfin un cryptage des données transitant entre le portable et l'entreprise devra lui aussi être imaginé, en même temps, qu'une signature électronique qui permettra d'authentifier les données. Cela pour éviter l'interception de trafic ou de signaux

3 - En ce qui concerne, le retour des commerciaux au sein de l'entreprise, seul une sécurité du poste de travail (le portable) et un paramétrage précis de ces derniers pourra protéger de façon sur et pas trop contraignante le réseau interne.

Nous pensons notamment à :

- La sécurité physique du poste : configuration du BIOS (mot de passe et boot impossible sur un autre disque) et mise en place de mot de passe fort à durée limitée sur le système d'exploitation
- L'installation d'une suite de logiciel de sécurité : Pare-feu, anti-virus, anti-malware, anti-spam
- La gestion des droits d'accès : mise en place de droits plus restreints pour les portables par exemple
- La minimisation des logiciels et services pour diminuer les vulnérabilités de ces PC plus exposés que du matériel fixe (notamment à cause de la connexion à partir de point divers : domicile, client, entreprise, hotel, hotspot ...)

Ce qui évitera les attaques physiques sur la machine pendant les déplacements des commerciaux, en effet, une personne pourrait placer un code malicieux au sein de la machine ou copier les données pendant que le commercial est occupé ailleurs. Mais aussi les attaques toutes sortes de virus ou autres espions.

2 – Architecture et service de sécurité

Résumons ce qui devra mis en œuvre :

- ✓ Un emplacement pour stocker les sauvegardes des données des PC portables
- ✓ Un concentrateur VPN pour l'accès des commerciaux depuis l'extérieur
- ✓ Un pare-feu au minimum pour sécuriser les réseau par des DMZ
- ✓ Configuration des postes de travail (voir ci-dessus point 3)
- ✓ Réduction des droits des commerciaux sur la gestion centralisée des utilisateurs

En effet, les commerciaux n'auront pas tous les droits sur leur machine pour limiter les menaces. Bien que cela soit un inconvénient car l'employé ne pourra installer et paramétrer sa machine comme il souhaite, cela reste indispensable. Surtout qu'il sera appelé à se connecter de plusieurs points différents.

Néanmoins, il faudra prévoir des droits suffisants pour qu'ils puissent configurer les différentes connexion (Hotel, Domicile, Client, etc ...)

3 - Solutions techniques

Pour cette mise en œuvre, beaucoup de choix devront être fait. À commencer par l'infrastructure actuel de l'entreprise :

- **Où placer le firewall ?**

Si il est unique, il devra être placé entre le modem et le reste du réseau.

- **Que placer au sein de la DMZ ?**

Les choix ici simple, chaque DMZ permettant d'isoler une ou des machines du reste du réseau, il faudra isoler le concentrateur VPN au sein d'une DMZ, le serveur Web au sein d'une autre DMZ, le serveur de messagerie et le proxy HTTP au sein d'une troisième DMZ et enfin le reste du réseau au sein d'une dernière DMZ. Cela dans un objectif de cloisement optimal.

Toujours dans un soucis de cloisement, chaque nouvel équipement devra être correctement installé, partitionné et configuré de façon judicieuse.

Un soin particulier devra être ensuite apporté sur le choix des protocoles d'authentification et de chiffrement. Ces derniers iront de pair avec le VPN, en effet, les deux choix seront liés. Il faudra choisir des protocoles compatibles entre l'infrastructure de l'entreprise (VPN) et le système utilisé sur les machines clients (PC portable).

Le protocole PPP associé à l'extension EAP pourrait être une bonne solution pour l'identification des commerciaux pendant leur déplacement.

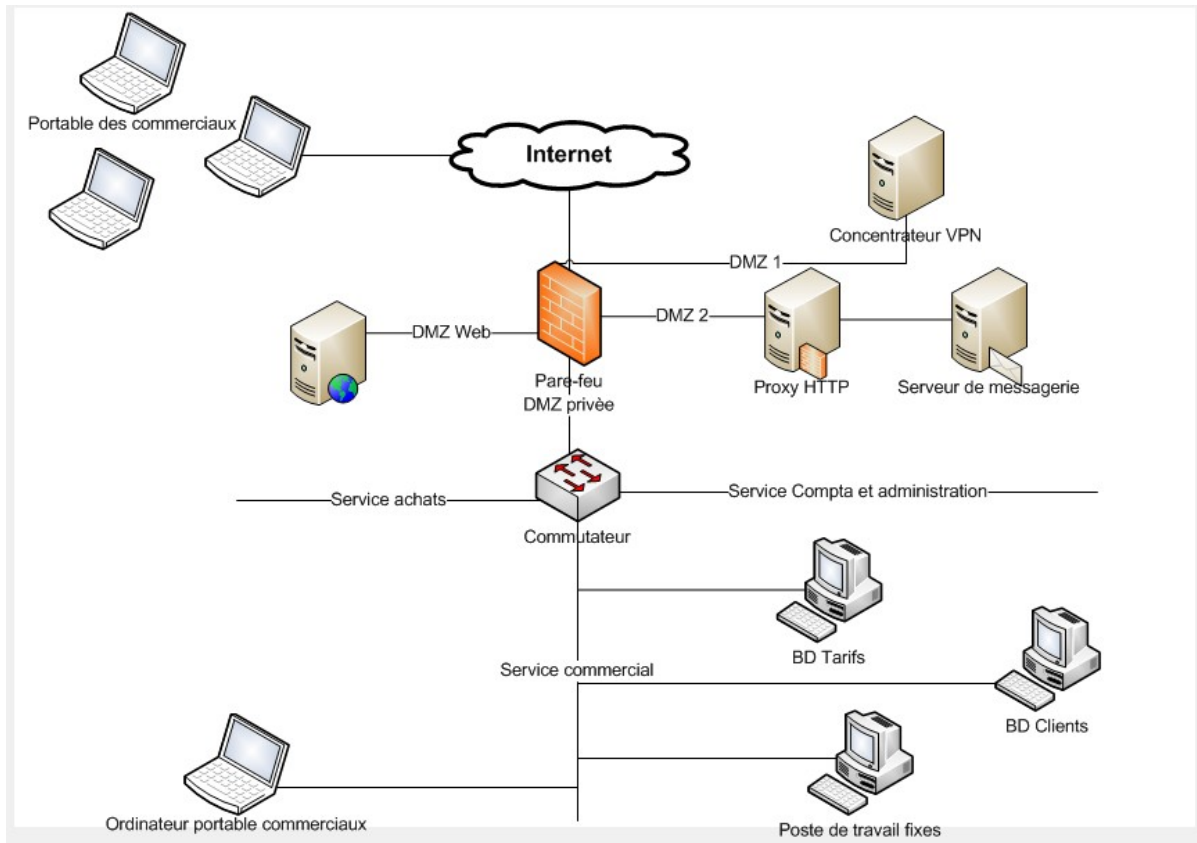
À ce propos, la question des OS linux, windows et mac OS devra être soulevée. Linux ayant de plus en plus de succès notamment pour sa sécurité améliorée est une solution qui devra être particulièrement bien étudié par l'équipe informatique. L'adoption des logiciels en découlera, en effet, tous les logiciels ne sont pas compatibles avec tous les systèmes d'exploitations.

Enfin, il ne faudra pas oublier les procédures et stratégies de suivi du matériel mais aussi des commerciaux qui pourront être sensibilisés tout au long de l'année aux problèmes de sécurités.

Au niveau du suivi des machines, une intention particulière devra être portée sur la mise à jour des logiciels et du systèmes.

Nous conseillerons d'une manière générale, à la société BIZ, de bien s'informer grâce notamment aux guides disponibles sur le site du Club de la Sécurité de l'Information Français (CLUSIF) mais aussi de ne pas négliger les certifications que pourraient proposer l'ISO ou l'organisme certificateur français LSTI.

Enfin, ils pourront s'aider des méthodes MEHARI, EBIOS, MARION pour analyser les systèmes de sécurités mise en place.



Voici une ébauche de schéma de ce que à quoi le réseau pourrait ressembler plus tard.