

UE 312 - Sécurité de l'Information

CIEL du 5 novembre 2008

- **Durée de l'épreuve: 2h, de 20:00 à 22:00 (heure de Paris).**
- **Le document est à DÉPOSER SUR LE SITE AVANT 22:00 (ressource CIEL 1 de l'UE 312). Un point de pénalité par minute de retard.**
- **Inscrire votre nom et votre prénom dans le document.**
- **En cas de problèmes, prévenir immédiatement PAR MAIL serge.bailly@unilim.fr ET rybowicz@unilim.fr. Les réclamations tardives ne seront pas prises en compte.**

Description du contexte: mobilité et sécurité

L'entreprise *Biz*, qui commercialise des jouets pour enfants fabriqués en Chine, envisage d'équiper ses commerciaux d'ordinateurs portables. L'entreprise est en bonne santé financière et en phase de croissance. Elle est d'importance nationale. Une centaine de commerciaux parcourent la France, démarchant clients et prospects. Elle dispose d'un petit service informatique de deux personnes doté d'un budget confortable lui permettant d'envisager d'acquérir du matériel et des logiciels, voire d'envisager un recrutement.

On cherche à analyser les risques liés à l'introduction de ces portables et à proposer des solutions visant à diminuer les risques.

Ces portables pourront être utilisés dans différents contextes :

- Ils pourront servir de poste de travail au sein de l'entreprise, lors des périodes où les commerciaux réintègrent les locaux de l'entreprise. Les portables pourraient alors remplacer les postes de travail fixes mis à leur disposition actuellement. Ces périodes sont régulières : environ une fois toutes les deux semaines, pour une présence sur site d'environ une semaine.
- Ils pourront être utilisés lors de déplacements chez des clients et connectés aux réseaux locaux des clients, si les entreprises clientes acceptent la connexion de visiteurs (en utilisant par exemple un serveur DHCP). Les réseaux des clients sont hors du contrôle de *Biz* et l'on ne peut pas faire d'hypothèse sur leur sécurisation.
- Les commerciaux pourront éventuellement les utiliser depuis leur chambre d'hôtel en utilisant le RTC (modem classique) et un compte chez un FAI, fourni par l'entreprise, ou par des accès Wi-Fi.

- Ils pourront être utilisés au domicile des commerciaux et connectés à Internet via le réseau téléphonique (ADSL ou modem classique).

Le réseau de *Biz* (voir le schéma du réseau en annexe) , *en l'état actuel*, est considéré comme raisonnablement sûr au regard des risques existants :

- les serveurs et postes de travail sont correctement installés, correctement configurés et mis à jour régulièrement par l'équipe informatique,
- le routeur filtrant est aussi correctement paramétré et ne laisse passer que le trafic entrant pertinent pour les activités de la société,
- les postes fixes sont munis d'un anti-virus automatiquement mis-à-jour.
- le proxy http relaie toutes les connexions Internet sortantes et un filtrage d'URL est mis en place pour éviter que le personnel ne perde trop de temps sur certains site sans rapport avec l'activité professionnelle,
- le personnel (fixe ou les commerciaux lors de leur séjour dans les locaux) accède aux bases de données via le réseaux local en utilisant des applications pas particulièrement protégées, mais le personnel est considéré comme loyal.

La société *Biz* étudie la possibilité de mettre à la disposition de ses commerciaux un certain nombre de services à partir de sa flotte de portables et elle souhaite que ces services soient accessibles dans un maximum de contextes. Les services sont :

- Messagerie électronique, pour communiquer avec l'entreprise et avec les clients.
- Accès Internet général (mappy pour le plan des routes, météo, sncf, etc...).
- Accès à une base de données «clients», l'informant sur le profil des clients (coordonnées, ristournes autorisées, historique de la relation client), avec possibilité de mise-à-jour par le commercial (compte-rendu de visite).
- Établissement de devis en ligne, avec possibilité d'impression chez le client (si autorisé par le client) ou de transmission au client par messagerie (et conservation d'un double). Pour l'établissement des devis, il faut pouvoir accéder à la base «clients» (pour les ristournes) et à la base «tarifs».

Le personnel de *Biz* est loyal, mais on ne peut pas exclure que certaines personnes soient tentées d'utiliser le matériel de l'entreprise à des fins personnelles : si une protection est en place, on pense que l'employé ne cherchera pas à la casser, mais si une utilisation à des fins personnelles est possible sans contrôle, elle risque fortement d'être exploitée. L'entreprise Biz est tolérante: si cette utilisation personnelle ne nuit pas à ses activités ou à sa sécurité, elle l'accepte.

1 Recensement des menaces et des impacts

Recenser les menaces supplémentaires que l'existence de ces portables peut faire peser sur le système d'information de l'entreprise. On s'intéressera notamment :

1. aux menaces sur les portables eux-même et les informations qu'ils sont susceptibles de contenir,

2. aux menaces portant sur les informations qui transitent entre les portables et l'entreprise, dans les différents contextes,
3. aux menaces portant sur les informations des serveurs de l'entreprise Biz (en particulier, du fait de la présence occasionnelle de machines portables sur le réseau local).

Pour chaque menace identifiée, on s'attachera à mesurer les impacts pour l'entreprise de la réalisation de la menace.

2 Architecture et service de sécurité

Comment mettre en oeuvre ces nouvelles fonctionnalités et quels services de sécurité peut-on proposer pour réduire les risques induits par les menaces ?

Remarque: on peut chercher à réduire un risque en limitant les possibilités de réalisation de la menace ou bien en diminuant l'impact de la réalisation de la menace....

On ne s'intéressera pas ici à des solutions techniques particulières, mais aux principes généraux et aux services de sécurité à fournir.

On pourra étudier les avantages et les inconvénients de conserver la maîtrise de l'administration et de la configuration des portables au niveau du service informatique.

3 Solutions techniques

Proposer une solution technique. On pourra éventuellement considérer les points suivants :

- infrastructure technique,
- choix de protocoles, éventuellement de logiciels ou d'OS,
- sécurisation des portables,
- modifications éventuelles du réseau local (on pourra s'aider d'un schéma, mais une description claire des modifications à mettre en oeuvre suffira),
- choix éventuels d'équipements complémentaires,
- développements logiciels spécifiques éventuels,
- points importants de configuration des équipements et des portables,
- procédures pour le déploiement du parc et des services,
- procédures pour le suivi du parc et de la sécurité de l'ensemble.
- ...