EXAMEN DE SECURITE INFORMATIQUE

Référence	ENSEEIHT 3AI – 2013-2014
Objet	Partiel de sécurité informatique
Auteur	M. Pierre-Yves BONNETAIN

CONTEXTE

L'entreprise ABC regroupe 250 collaborateurs, sur un seul site. L'illustration 1 présente l'architecture du réseau interne de l'entreprise. Celui-ci est construit autour d'un ensemble de commutateurs (switches), sur lesquels tous les ordinateurs (postes de travail et serveurs) sont connectés. Un routeur, relié au commutateur, sert de point de sortie vers Internet.

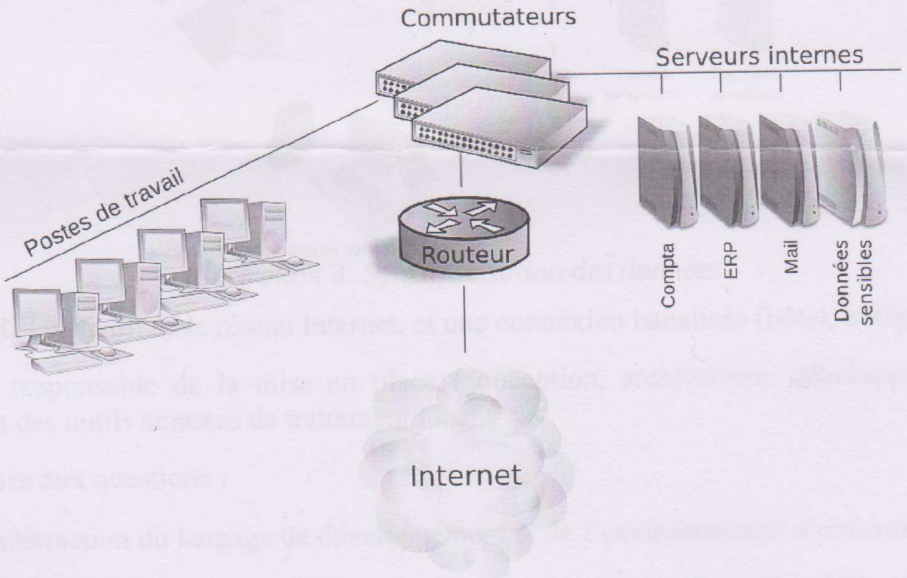

Illustration 1: Réseau interne de ABC

Parmi les projets majeurs de l'entreprise, celle-ci souhaite permettre à ses commerciaux (une dizaine de personnes, mobiles sur toute la planète) d'accéder au système (interne) de suivi des clients (l'ERP). Cet outil contient des informations très sensibles pour l'entreprise (suivi des prospects en cours de négociation, rabais accordés, suivi des contrats, etc.). L'illustration 2 présente l'architecture logique de l'outil existant.

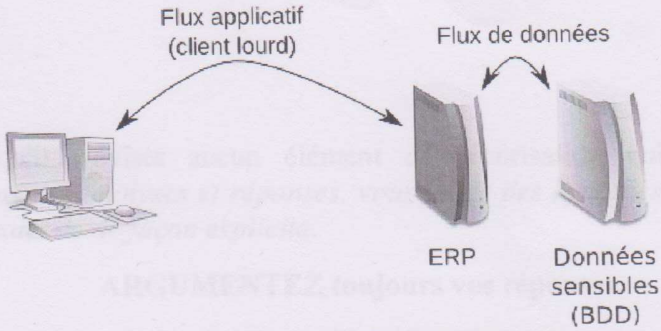

Illustration 2: Flux applicatif et données

Le commercial doit pouvoir travailler sans être connecté à l'entreprise. S'il est déconnecté, les modifications sont stockées localement sur le poste de l'utilisateur, et reportées sur le système central à la connexion suivante. S'il est connecté, la mise à jour est faite en parallèle sur les données locale et sur le système central. L'illustration 3 présente succinctement cette situation.

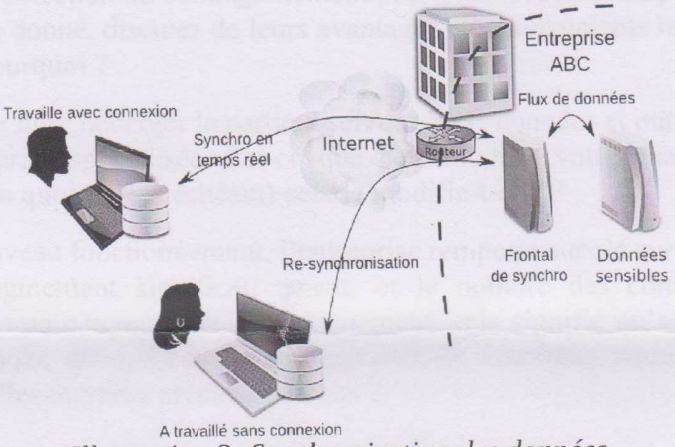

Illustration 3: Synchronisation des données

L'accès à distance utilise le réseau Internet, et une connexion banalisée (hôtel, hotspot Wifi, etc.).

Vous êtes responsable de la mise en place (conception, architecture, développement) de ce programme et des outils annexes de traitement local.

Les réponses aux questions :

- Font abstraction du langage de développement et de l'environnement d'exécution.
- Ne concernent que la sécurité du système, pas ses fonctionnalités opérationnelles.
- Font notamment abstraction des problèmes de mise à jour parallèle de la même information par des commerciaux différents.
- S'affranchissent des contraintes économiques (coûts et délais).

QUESTIONS

Nous supposons qu'il n'existe aucun élément de sécurisation qui ne serait pas décrit précédemment. *Si, dans vos analyses et réponses, vous faites des hypothèses quant à ce qui existe ou devrait exister, signalez-le de façon explicite.*

ARGUMENTEZ toujours vos réponses.

1. Indiquez les principaux risques que vous identifiez par rapport au système d'informations de ABC et au projet de travail à distance, en **expliquant/argumentant votre choix**. Classez ces risques (en signalant s'il s'agit d'un classement par importance croissante ou décroissante).

2. Pour les trois principaux risques identifiés à la question précédente, discutez des mesures de prévention, de détection ou contingentement possibles. Si plusieurs possibilités existent pour gérer un risque donné, discutez de leurs avantages et inconvénients respectifs. Quels seraient vos choix et pourquoi ?

3. ABC décide de faire héberger la partie « serveur ERP, données et outils de synchronisation » par une entreprise spécialisée. Est-ce que cela modifie votre analyse des risques de la question 1 et en quoi (le cas échéant) cela la modifie-t-elle ?

4. Grâce à ce nouveau fonctionnement, l'entreprise remporte succès sur succès. Les effectifs de l'entreprise augmentent significativement, et le nombre des commerciaux passe d'une dizaine à plus une cinquantaine. Statistiquement, cela signifie qu'au moins un portable va être perdu chaque mois. Cela fait-il apparaître de nouveaux risques ? Si oui, lesquels ? Quelles nouvelles mesures préconisez-vous ?