Examen TIW4

Sujet d'examen individuel du jeudi 16 décembre. Durée 1h30.
Tous documents et supports autorisés. Le barême est indicatif.

1 Cas d'étude

On considère le cabinet d'avocats, *Alain Mateur & Associés*, spécialisé en droit des sociétés et droit des affaires. Les clients du cabinet sont des entreprises dont la taille varie d'une dizaine d'employés à plusieurs centaines. Le personnel du cabinet est composé :

- de 6 associés, des avocats qui détiennent des parts du cabinet ;
- de 10 collaborateurs, des avocats salariés du cabinet qui n'en détiennent pas de parts ;
- de 16 assistants, des juristes qui ne sont pas avocats. Il y a un assistant par avocat, qui travaille sur les dossiers confiés à ce dernier ;
- de 16 secrétaires, un par avocat ;
- de l'administrateur informatique et ses deux assistants.

Tous les collaborateurs sont en contrats à durée indéterminés. En revanche, environ la moitié des assistants et un tier des secrétaires sont salariés pour une durée déterminée.

Le cabinet dispose d'un système informatisé de gestion des affaires qu'il traite, développé par un stagiaire. Le stagiaire a depuis quitté la structure dans des conditions tumultueuses, suite à un conflit personnel. Actuellement, le système de gestion ne dispose pas de contrôle d'accès fin : tous les personnels ont un accès complet. Le système de gestion du cabinet est une application PHP/MySQL qui permet de gérer les activités essentielles du cabinet à savoir :

- la prospection de sociétés,
- la gestion des affaires civiles et des affaires pénales des sociétés clientes,
- la facturation des honoraires aux clients,
- la gestion des affaires contre le cabinet.

Chaque avocat dispose d'un ordinateur portable et d'un ordinateur de bureau. Chaque assistant et chaque secrétaire dispose d'un ordinateur de bureau. Les assistants utilisent souvent leurs ordinateurs portables personnels.

Le cabinet utilise un serveur sur lequel tourne un service Apache et le système de gestion de base de données MySQL. C'est l'unique serveur du cabinet. Il hebèrge l'application de gestion. Les configurations des services `sendmail`, `apache`, `mysql` et `ftp` sont quasiment celles par défaut. Le serveur `ftp` n'est en fait plus utilisé depuis 2005.

Les machines fixes et le serveur sont reliés en réseau ethernet. Un réseau wifi est disponible pour les machines nomades. L'accès Internet est assuré par une liaison ADSL reliée à l'unique routeur du cabinet. Le routeur dispose également de capacités de filtrage niveau IP uniquement. Toutes les machines fixes, nomades et le serveur sont dans un même sous-réseau privé.

L'ensemble du système d'information du cabinet est administré par le beau-frère d'Alain Mateur, chimiste de formation, et ses deux assistants. Actuellement, pour des raisons de facilité d'utilisation et d'administration, le serveur d'application est accessible depuis l'extérieur, les machines nomades se connectant par Internet. Les postes fixes sont gérés par l'administrateur. En revanche les machines nomades sont à la totale disposition de leurs utilisateurs.

2 Analyse générale du système

Le cabinet commande un audit de l'état de la sécurité de son système, redoutant une malveillance de la part de l'ancien stagiaire. On limitera le champs de l'étude aux affaires des sociétés clientes (on ne s'interesse pas aux autres processus métier).

Question 2.1 (4pts) Dégager *méthodiquement* les risques intolérables auxquels est exposé le cabinet. On pourra préalablement identifier les principales sources de menances, les principaux événements redoutés et les scenarii de menace selon la méthode EBIOS.

Question 2.2 (2pts) Proposer des mesures *organisationnelles et humaines* pour réduire ces risques (les mesures techniques sont considérées en section suivante).

3 Mesures techniques

Le stagiaire qui a developpé l'application de gestion a utilisé l'abominable extrait de code suivant pour gérer l'authentification :

```
1  $username = $_GET['username'];
2  $password = $_GET['password'];
3  $sqluser = mysql_query("SELECT COUNT(*) FROM users WHERE username = '".$username."'"
       );
4
5  $countuser = mysql_fetch_row($sqluser);
6      if ($countuser[0] == 0) {
7          $errormsg = "Your Username is incorrect. Please try again";
8      } else {
9          $sqlpass = mysql_query("SELECT COUNT(*) FROM users WHERE username = '".
               $username."' AND password = '".$password."'");
10         $countpass = mysql_fetch_row($sqlpass);
11         if ($countpass[0] == 0) {
12             $errormsg = "Your Password is incorrect. Please try again";
13         } else {
14             $page = $_GET['page'];
15             if (file_exists('pages/'.$page.'.php')) {
16                 include('pages/'.$page.'.php');
17                 ...
18             }
19         }
20     }
```

Question 3.1 (3pts) Proposer une nouvelle gestion de l'accès au réseau des postes nomades. On différenciera la gestion des accès depuis le réseau interne des accès depuis l'extérieur du cabinet. Accompagner la proposition de mesures techniques.

Question 3.2 (2pts) Proposer une nouvelle organisation de l'architecture matérielle et logicielle du serveur qui offrirait une meilleur sécurité.

Question 3.3 (4pts) Identifier différentes failles de sécurité logicielles de l'authentification de l'application de gestion. Proposer des mesures correctives (le détail du code n'est pas demandé).

4 Contrôle d'accès

Question 4.1 (5pts) Proposer une politique de contrôle d'accès de type RBAC pour contrôler les accès à l'application de gestion. Le modèle peut éventuellement être étendu pour prendre en compte les spécificités du métier du cabinet.