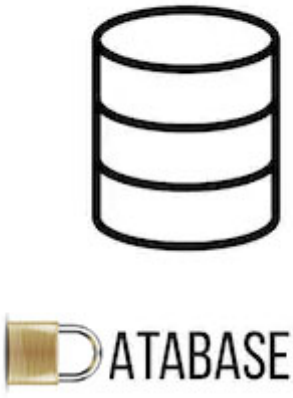
Sécurité des données : évaluation finale

Année académique 2018-2019

Rapport théorique



Sous la direction de M. Bob MULUMBA et M. Mohamed BOURAADA, professeurs de sécurité des données.

Rapport de deuxième année de bachelier à l'henallux, dans l'option sécurité des systèmes.

Descamps Ludovic, Thomas Matis

Table des matières

1 Violations au niveau de la sécurité dans la base de données interne

Il y a eu plusieurs brèches de sécurité dans la société, qui ont mené à :

1. Une société **concurrente** a obtenu des informations personnelles de plusieurs clients de la société.
2. De nouveaux employés ont *accidentellement* révélé des informations *critiques, et donc confidentielles*, en les envoyant par **email** à leurs connaissances.
3. Plusieurs suppressions *accidentelles* de données **sans** possibilité de **restauration**.

2 Causes potentielles des défaillances de sécurité

2.1 Liées à la confidentialité

a. Il n'existe aucun système de **gestion d'utilisateurs** : chaque employé a accès à toutes les données. Or, le stagiaire de l'entreprise ne doit pas avoir les mêmes accès aux bases de données que l'administrateur de celles-ci !

b. Les informations personnelles des clients de DLS ont donc été récupérées par une société concurrente, soit via un utilisateur *de manière volontaire ou non* en interne, soit la société concurrente à réussi à pénétrer dans le système de DLS.

c. Les nouveaux employés ayant accès à toutes les données, ne peuvent pas facilement distinguer les informations sensibles des autres.

2.2 Liées à la disponibilité

a. Il n'y a aucune restriction d'accès aux données. Il serait nécessaire de **restreindre l'accès** aux données à un environnement sécurisé et aux heures de bureau.

2.3 Liées à l'intégrité

a. Il n'y a aucune vérification quant à la modification ou suppression des données.

b. Les modifications de la base de données ne sont pas monitorées. La BDD n'est donc pas intègre : chacun pourrait, par exemple, supprimer un collègue de la base de données et le faire disparaître de la société.

2.4 Liées à la non-répudiation, ou tracabilité

a. Il n'y a aucune trace de l'état et des mouvements des données. Il n'existe aucun historique et on ne peut pas suivre ce qu'il s'est passé sur la BDD.

b. Sans traçabilité, on ne peut pas s'assurer que les 3 critères précédents sont respectés. La tracabilité aurait permis ici de savoir comment la société concurrente s'est emparé des données des clients de DLS, et de savoir quel employé commet quelle erreur dans la BDD.

3 Solutions de sécurité proposées à la société

3.1 Centrées sur la confidentialité

3.1.1 Filtrage

Filtrer les informations sortantes. Par exemple, il est possible de bloquer les mails sortants qui contiennent des mots-clefs prédéfinis, même si ces mots-clefs sont contenus dans la pièce jointe. Si un mail est bloqué, notifier un administrateur en lui donner le contenu du mail ainsi que l'adresse mail et l'utilisateur qui l'a envoyé.

3.2 Centrées sur l'intégrité

3.2.1 Backups

Créer des **backups** complets des bases de données, automatisés et gardant différentes versions de ceux-ci, et mettre en place les normes de conservations de backups, ainsi que les protocoles et tests de récupération. [1]

3.2.2 RAID

Installer les bases de données sur un système RAID avec redondance : par exemple le RAID1 ou le RAID5 (meilleures performances et possibilité d'utiliser un spare disk).

3.3 Centrées sur la disponibilité et l'intégrité

3.3.1 UPS

Installer un UPS [2] afin d'éviter toute corruption des bases de données suite à une panne électrique, et garantir la disponibilité des services.

3.4 Solutions générales

3.4.1 Bases de la sécurité informatique

Renforcer (ou mettre en place) les **bases de la sécurité** au niveau des postes de travail, telles que : installer un firewall, installer un antivirus, mettre en place des mots de passe robustes, et faire régulièrement les mises à jour.

3.4.2 Administration des droits

Créer un Active Directory afin d'instaurer et d'**administrer** les droits d'accès.

3.4.3 Journalisation

Mettre en place un procédé lors de la modification ou la suppression de données, qui permettra d'identifier le compte l'ayant réalisée : mise en place d'un système de journalisation.

1. `https://wordpress.com/view/securiteinformatiquepourdebutants.wordpress.com`
2. Uninterruptible Power Supply

3.4.4 HTTPS

Au niveau du site web, toujours utiliser le protocole **https** et non http, pour des raisons évidentes de sécurité, telles que crypter les données sensibles qui sont échangées entre le serveur et les clients.

3.4.5 Injections SQL

Interdir les injections SQL. L'injection SQL se produit lorsque des commandes SQL sont introduites dans les champs à remplir pour s'identifier par exemple. Imaginons que le code de la requête soit le suivant :
`select * from data where login = '$login' and password = '$password'`
Dans ce cas, si un utilisateur connait un login et remplit le champ password avec ceci : `' or 1 = 1 - -` , la requête finale sera celle-ci : **select * from data where login = '$login' and password = '' or 1=1 - -'**

donc la condition du mot de passe sera vraie, et il pourra accéder à ce compte sans connaître le mot de passe. Plus grave encore, il pourrait ajouter d'autres commandes dans le champ mot de passe et **supprimer/modifier/ajouter/lire** toutes les données de la base de données. C'est arrivé de nombreuses fois.
Il faut informer les programmeurs au niveau du service web afin qu'ils protègent l'entreprise de ces injections. [3], et imposer l'utilisation de **requêtes préparées** : prohiber les requêtes dynamiques, et passer les variables en paramètre. [4]

3.4.6 Limite de tentatives d'accès

Mettre une **limite de tentatives d'accès** aux bases de données et à l'authentification sur le site web pour éviter le bruteforce, dictionary attack, etc. Une fois que cette limite est atteinte, désactiver le compte de l'utilisateur, qui ne pourra le réactiver qu'après avoir saisi un code qui lui sera envoyé par mail.

3.4.7 GDPR

Respecter le **GDPR** (Règlement Général sur la Protection des Données) [5] : ne pas respecter ce règlement pourrait mettre en péril la société : les sanctions sont lourdes, et mettraient également en péril la disponibilité des services. En effet, l'amende pourrait s'élever à 4 % du **chiffre d'affaires** de l'entreprise. e.g. : Informer et obtenir le consentement des utilisateurs du site web sur l'utilisation de leurs données personnelles. [6]

3.4.8 Formation et sensibilisation à la sécurité informatique

Former et sensibiliser les employés et les utilisateurs des bases de données à la sécurité informatique, plus particulièrement de ces bases de données. En effet, les failles exploitées sont bien plus souvent humaines que logicielles.

3. https://www.leblogduhacker.fr/se-proteger-de-l-injection-sql/
4. http://php.net/manual/fr/function.mysql-real-escape-string.php
5. RGPD en français. En anglais, les initiales GDPR signifient General Data Protection Regulation
6. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679