




Éditorial

Bases de données et sécurité ...

Louis Nyffenegger 

Les bases de données sont souvent le lieu de stockage des informations importantes et sensibles de l'entreprise. Paradoxalement, ce sont aussi souvent le maillon faible de la sécurité d'une entreprise. En effet, elles sont directement au cœur du système d'information, et leur arrêt, redémarrage ou le moindre risque d'interruption de service n'est pas envisageable pour les équipes de production. Ce maintien de la disponibilité se fait évidemment au détriment de la sécurité du serveur de base de données et donc de l'intégralité du système d'information de l'entreprise.

Pour une personne réalisant une intrusion, une base de données peut être compromise de trois façons : directement en accédant à la base de données, via le système d'exploitation hébergeant le service ou via une application utilisant cette base de données.

Pour les deux premières méthodes, c'est souvent le manque de mises à jour de l'hébergeur du service (le système d'exploitation) ou du service lui-même qui permet de compromettre la base de données.

En effet, on assiste souvent à des absences de durcissement de ces systèmes : comptes triviaux au niveau de la base de données (*scott/tiger, dba/dba, snmp/snmp, sa/, root/*) ou au niveau du système (*oracle/oracle, root/root*), absence de mise en place des correctifs avant la mise en production ou depuis la mise en place, absence de durcissement de la machine hébergeant la base de données ou de la base de données elle-même (suppression ou restriction des accès à certains paquets comme *UTL_**, mise en place d'un mot de passe sur le *listener*) ...

Souvent, ce sont les fonctionnalités non nécessaires, et donc qui auraient pu être désactivées, qui sont à l'origine des problèmes de sécurité. Un paramétrage *sécurité par défaut* basé sur une installation minimaliste devrait plus souvent être mis en place par les fournisseurs de bases de données.

Par exemple, Oracle est une référence dans le domaine des bases de données, avec des fonctionnalités très évoluées qui ne sont en général utilisées que par les pirates, celles-ci devraient être désactivées par défaut.

De plus, la multiplication des outils périphériques au SGBD : interface de consultation, gestion d'accès en

Webservices sont tout autant de nouveaux points d'accès potentiels vulnérables aux données hébergées.

Malheureusement, ce type d'attaques provenant majoritairement de l'intérieur, elles ne sont pas toujours prises au sérieux par les responsables de sécurité, le fait que ces bases de données ne soient pas accessibles depuis Internet leur suffit. Dans la réalité, lors d'intrusion interne, on se rend vite compte que c'est le point sensible, là où les données importantes sont présentes. La base de données est ensuite un bon point de départ pour rebondir dans l'entreprise.

L'attaque au travers d'une application est plus problématique, car souvent mise en place sur des applications exposées à Internet. Même si les attaques de type injections SQL sont connues depuis plusieurs années, des milliers d'applications sont encore et toujours vulnérables à ce type d'attaque. De plus, les techniques d'injection sont de plus en plus poussées et l'exemple de renvoi de données par DNS [1] lors d'une injection à l'aveugle montre bien jusqu'où un attaquant motivé peut aller.

La sécurité des bases de données a aussi vu naître dernièrement une nouvelle spécialité : l'étude post-incident sur les bases de données. En effet, deux présentations ont ainsi été réalisées à BlackHat : *Database forensics* [2] par David Litchfield et *SQL Server Database Forensics* [3] par Kevvie Fowler.

Il y a donc fort à parier que les bases de données ne seront pas avant longtemps *unbreakables* comme certains ont pu l'annoncer.

- [1] <http://www.inspectit.se/dc15.html>
- [2] <http://databasesecurity.com/database-forensics.htm>
- [3] <https://www.blackhat.com/presentations/bh-usa-07/Fowler/Presentation/bh-usa-07-fowler.pdf>

À propos de l'auteur

Louis Nyffenegger est consultant en sécurité suisse travaillant chez HSC (*Hervé Schauer Consultants* – <http://www.hsc.fr>). Il réalise des audits, études et tests d'intrusion. Louis remercie toute l'équipe HSC pour son aide et les relectures. Louis peut être contacté à l'adresse suivante : Louis.Nyffenegger@hsc.fr.