www.silensec.com

# Threats and Vulnerabilities to Corporate Databases

silensec©
Since 1998

02.

In every organization today, databases hold the crown jewels, hosting anything from client information to personnel files.

Every cyber attack, whether from internal or external users is aimed at gaining unauthorized access to sensitive data stored inside corporate databases. Also, most business services today are delivered through the Web and the most serious attacks to Web applications themselves are aimed at gaining unauthorized access to the underlying database technologies. Unfortunately, many organizations do not give adequate attention to securing their corporate databases and many attacks and misuse go unnoticed until it is too late. In order to understand how to protect corporate databases, it is important to thoroughly understand the range of weaknesses and threats that are challenging such vital technology.

To begin with, let's discuss the most common threats, i.e. what could happen to a database that was not appropriately secured. The consequences are most commonly information disclosure, disruption to business operation, financial loss and loss of image and reputation.

## 1 Misuse of Privileged Accounts

Databases, like any system, requires the use of privileged accounts to perform daily tasks such as user management, performance tuning, replication, patching, backup etc. Also, like any other system, the use of such privileged accounts needs to be monitored to ensure that the associated users do not abuse their privileges to gain unauthorized access to sensitive information or to execute unauthorized tasks such as adding new users to the database or granting unauthorized privileges to other users. Besides intentional misuse, there is another important reason why privileged accounts must be monitored. Given the rights that privileged accounts have, they are the prime targets of attackers who know that, by compromising any such account, can easily gain access to the entire database.

## 2 Privilege Abuse

This threat applies to all accounts, not just the privileged ones and refers to the use of a database account rights beyond what that account is allowed or meant to do. A classic example is the privilege abuse associated to call centre users who access a CRM. Access to the CRM is via a Web interface that allows to bring up only one customer record at a time, preventing the user from viewing multiple customer records at the same. However, using the same user account and a different database client, as simple as MS Excel, it is possible to abuse the given privilege and export as many customer records as possible onto a portable USB drive. A common way of abusing privileges is via SQL Injection attacks where the attacker inserts SQL statements into the input fields of web applications that fail to perform input validation.

## 3 Exploitation of Vulnerabilities

While the previous threats are related to the misuse and abuse of database account privileges (i.e. someone must have already gained access to the database), the most common threat to databases is direct attacks to the database trying to enumerate and exploit existing vulnerabilities. Vulnerabilities, as described later in this paper, can come from unapplied security patches, misconfiguration, weak passwords and more. If a database is left vulnerable and without protection it is to be expected that it will be attacked and that one of the existing vulnerabilities may be exploited.

### HOW TO SECURE YOUR DATABASES

Choosing the right security technology and products to secure your databases is not easy. Every organization is different and acquiring a security product is not enough. Every solution needs to be carefully designed to address the specific needs of the organization, icluding database technologies used, data to be protected, business processes to be integrated and last but not least the staff competence. No product will run by itself and security will always rely on the competence of users!

silensec©
Since 1998

03.

Understanding the threats helps in appreciating the importance of securing databases

Understanding the threats helps in appreciating the importance of securing databases but what are the most common vulnerabilities that are normally found in databases, and what weaknesses are malicious users looking for and trying to exploit? The following is the list of the most common vulnerabilities undermining the security of databases.

## 1 Weak Passwords

Password attacks are amongst the most common attack vectors carried out against databases. Password attacks are likely to yield a good number of user passwords belonging to both privileged and unprivileged users. Along with misconfiguration and lack of security patches, weak passwords are among the top three weaknesses affecting the security of databases. Strong password management and password use must be enforced and audited across all corporate databases, beginning from changing the default passwords during database installation.

## 2 Unapplied Security Patches

As much as it may sound obvious, this is also a common vulnerability that exposes databases to unauthorized access. Compared to other common vulnerabilities, patching is the most challenging one to tackle. Databases, like operating systems, eventually reach End of Life (EOL), after which the vendor stops issuing patches to fix new-found vulnerabilities. In that case the organization has two possible options: leave the system unpatched and exposed or upgrade to the latest version of the database. In most cases, the latter option is easier said than done as it brings along issues of database migration, downtime, redevelopment and testing of legacy applications that had been built on the old database etc. Even if the database has not reached the EOL, the patching process always has to ensure minimal disruption of business services.

Misconfiguration, whether intentional or unintentional, is one of the top three vulnerabilities that lead to unauthorised access to databases.

## 3 Database Misconfiguration

Examples include changes to database structures such as application tables and roles, changes of privileges, ad hoc creation of new database accounts. It is easy to see what any of those types of misconfigurations could lead to. The following vulnerabilities are the most critical ones related to database misconfiguration:

a. **Misconfigured Privileges**
   Just like any other system, databases required user accounts to be accessed and operated. Over time, users with different privileges are created based on business needs and to deliver specific services. As business requirements changes and as people's roles and responsibilities also change, there is a need to always ensure that only the required privileges are granted in order to reduce to abuses. Understanding the set of unused roles and privileges is important because it helps running the database with the minimum required privileges thus reducing the opportunity of privilege abuse or misuse.

b. **Unnecessary Access to Sensitive Data**
   Many databases contain personal identifiable information (PII), personal sensitive data or commercially sensitive data. Access to such data is required in order for the business to be able to deliver its services. However, in many cases what is needed is not the entire record but only the part that is used within the business process. For instance, in order to validate a customer's identity and access rights to a service (e.g. authorizing a bank transaction) a call center operator does not need to have access to the customer's full set of security identification information, which may be misused to impersonate the customer. In most cases, access to the database is through a Web interface that takes care of hiding sensitive information. However, such protection is also required directly on the database to prevent cases of privilege abuse.

## 4 Weak Database Logging

Since databases contain data of varying degrees of sensitivity, collecting database logs is not only important to be able to investigate abuses and attacks but it is also a mandatory requirement for a number of international standards and regulations. While databases include native logging and audit capabilities, challenges arise when different database technologies from different vendors need to be integrated. Ensuring a strong database audit trail goes beyond the technical aspects and the organization must also address issues of data retention, data disposal and reporting along with the associated roles and responsibilities.

While the threat scenario may not be a pretty picture to look at and despite managing database vulnerabilities may not be an easy task, especially when dealing with a wide range of vendors and technologies, a lot can be done to ensure that sensitive data is appropriately protected. Key technologies to consider for the protection of databases include: database vulnerability scanners, database activity monitoring, database firewalls, data masking, virtual patching and database encryption. Which technology to deploy, how to use it and which vendor to buy it from are some of the critical questions an organization must answer. However, whether databases require adequate security or not, is out of the question!

### About the Author

Almerindo Graziano is the CEO of Silensec. He holds an MSc in Electronic Engineering and a PhD in mobile security, both from the University of Naples, Italy. His areas of expertise include security standards compliance, corporate infrastructure protection, design of SIEM and Log Management systems and development of security monitoring processes for effective and efficient incident response.