Whitepaper

The Need for Real-Time Database Monitoring, Auditing and Intrusion Prevention

May 2007

© Copyright Sentrigo Ltd. 2007, All Rights Reserved
The Challenge: Securing the Database

Much of the effort in recent years to secure the corporate IT infrastructure has focused on the perimeter – how to defend the enterprise from external intruders, from hacking and from malicious attacks. Then, the corporate network has seen its share of improvements in its security, providing a further layer of protection. The data layer, however, has remained the soft underbelly of enterprise IT infrastructure.

Databases hold much of the most sensitive and valuable data – information about customers, transactions, financial performance and human resources to give a few examples. Despite this, databases remain one of the least protected areas in the enterprise. While perimeter and network security measures create a barrier against some type of attacks, there are attack patterns that take advantage of database-specific vulnerabilities.

SQL injection, buffer overflow attacks and other “zero-day” hacks can cut right through Web firewalls, application firewalls and intrusion detection systems (IDS) and create opportunities for data theft, unauthorized modification or destruction of data, or breaches of privacy and personally identifiable information.

Since database management systems are complex, supporting an ever growing set of requirements and platforms, with addition of features they develop gaps in security – vulnerabilities – that are constantly being discovered by users, ethical hackers and unfortunately, non-ethical hackers as well. Such vulnerabilities are reported to DBMS vendors who do their best to patch them, but this is a process that currently takes several months on average, and in some cases years. That time lag is essentially an open invitation to exploit the vulnerability and breach the database.

Additionally, there is growing recognition that the “insider threat”, and specifically the threat posed by users with privileged access, is responsible for a large number of data breaches. According to annual research conducted by CERT, up to 50% of breaches are attributed to internal users. The 2006 FBI/CSI report on the insider threat notes that two thirds of surveyed organizations (both commercial and government) reported losses caused by internal breaches, and some attributed as much as 80% of the damage to internal breaches. It was also reported that 57% of implicated insiders had privileged access to data at the time of breach. It is therefore evident that perimeter and network security measures are not enough to stop such breaches.

Finally, legislation and regulatory requirements such as Sarbanes Oxley for public companies, HIPAA in healthcare, GLBA in financial services and the credit card industry’s PCI DSS all mandate that companies and organizations take certain measures to ensure the privacy, integrity and security of sensitive data.

The evolution of security threats vis-à-vis the existing infrastructure paint a clear picture – databases need protection on a granular, intimate level, using solutions that can handle database-specific threats on the one hand, and deal with the insider threat on the other hand.
Existing Database Security Tools

There is a wide array of technologies currently in use for securing databases. As with other areas of IT security, no single tool can provide ironclad defense against all threats and abuses. It is always recommended to employ a combination of tools to achieve adequate security.

Identity Management and Access Control

**PROS:** Establishes roles and privileges, the most basic level of security

**CONS:** Difficult to enforce properly, over-liberal granting of access, open to hacking, privileged users have free reign

The ability to designate roles, logins and passwords is the most basic level of database security, and used pretty much everywhere. Unfortunately, it is very common within enterprises to have group usernames and passwords and to forget to revoke privileges of employees who no longer need them. This mechanism is also exposed to hacking (e.g., SQL injections that escalate privileges).

Native Database Audit Tools

**PROS:** Provide granular audit trail and forensics of database activity

**CONS:** Serious database performance impact, only after-the-fact forensics, no prevention capabilities, no separation of duties, easy to turn off

Most DBMSs come with a set of features that enable granular auditing of every single database activity. However, these features are seldom used because of the negative impact they have on performance. Furthermore, because they are part of the DBMS, they are administered by DBAs in a way akin to “letting the cat guard the cream”.

Encryption

**PROS:** Protects sensitive data

**CONS:** Key management overhead, performance impact, difficult to manage

Column-level or table-level encryption within the database ensures that sensitive data such as credit card numbers cannot be viewed by users having general access to the database (e.g. via a CRM application). However, encryption alone is insufficient, because it is often decrypted for communication with applications, and this creates an opportunity for accessing the encrypted data. It is also impractical to encrypt all data due to performance issues and key management overhead, so unencrypted data remains vulnerable.

Monitoring using Network Appliances

**PROS:** Provide alerts (and if used in-line, prevention) on network access to the database

**CONS:** Do not protect against insiders with access privileges / local access, require network reconfiguration, if used in-line slow create network bottleneck, cannot handle encrypted traffic, expensive hardware

This is a class of network-based appliances, which monitor network traffic looking for SQL statements, and analyze the statements based on policy rules to create alerts on illegitimate access to the database and attacks. Because the appliance are only monitoring the network, they do not have visibility into local database activity, essentially leaving the database vulnerable to
insiders that either have local access or are savvy enough to bypass the appliances. In order to provide adequate monitoring, the appliance must be deployed at every choke point on the network where the database is accessed, encircling the database from all sides. For mission-critical databases that are often tied into a multitude of applications (ERP, CRM, BI, billing etc.), this significantly raises the cost, which is high to begin with.

**Hedgehog - Real-Time Database Monitoring and Intrusion Prevention**

Sentrigo’s Hedgehog is an elegant software solution for database security. It is a system that monitors all database activity in real-time, and based on a defined rules and policies issues alerts on suspicious activity and, if necessary, stops it as it happens.

Hedgehog is comprised of a small footprint sensor, a software agent that is installed on the database host server itself and monitors all activity. It is nonintrusive, easy to install and consumes only small amounts of CPU resources (<5% of a single CPU, even on multi-CPU machines). The sensor communicates with the Hedgehog server, which generates alerts according to the defined rules.

The policy rules apply to types of SQL statements, database objects, time of day or day of the month, specific user profiles and the applications used. The action taken when the conditions of a rule are met can be as simple as logging an event, sending an alert to a SIM/SEM system, via e-mail or SMS, or terminating a user session to prevent malicious activity. The system comes with predefined rules that prevent known attacks that exploit database vulnerabilities.

A single Hedgehog server can manage and communicate with numerous sensors on different databases, and an enterprise installation can easily scale up to encompass hundreds of databases. The server also easily integrates with IT infrastructure to facilitate central IT management and security event management.
Since the Hedgehog sensor is installed on the database machine, it is impossible to bypass and possesses self-defense mechanisms that alert on any tampering attempts. The structure of the system also ensures separation of duties, a key requirement in IT security. The Hedgehog administrator, the person defining policy rules and the person receiving alerts can all be different people in different departments within the organization (for example, IT manager, DBA manager and CISO respectively).

Sentrigo employs a “Red Team”, a group of ethical hackers who are on the lookout for new database vulnerabilities. As soon as such vulnerabilities are discovered, the team creates rules that protect against them – essentially virtual patches that immediately protect the database without the need for a system upgrade or downtime, and leaving the database exposed until DBMS updates are issued by the vendor.

**Unique Advantages:**

- The only database monitoring solution that monitors all database activities and provides protection against insiders with privileged access
- Granular monitoring of database transactions, queries, objects and stored procedures, with real-time alerts and prevention of breaches
- Flexible rules that allow enforcement of corporate security policy with minimal “false positive” alerts
- Virtual patching of newly discovered database vulnerabilities, providing immediate protection with no DBMS downtime
- Flexible audit and reporting capabilities
- An easy-to-deploy and scalable software solution
- Separation of duties