Ten Database Activities Enterprises Need to Monitor

Gartner RAS Core Research Note G00200212, Jeffrey Wheatman, 28 April 2010

Most enterprises are paying too little attention to the very real security risks associated with their databases. Auditors, security and risk professionals, and data owners need to watch for telltale behaviors that may indicate serious database security problems.

Key Findings

- The use of structured data storage, and the amount of data stored in this way, are increasing rapidly. This trend is largely driven by data analytics requirements and consolidation efforts.
- The information stored in enterprise databases is increasingly sensitive and subject to legal, regulatory and other compliance requirements.
- Despite the growing criticality of their databases, many enterprises continue to rely heavily on inadequate network and application-layer controls, and perform only minimal monitoring on database storage infrastructure.

Recommendations

- Evaluate your enterprise's current database controls to identify gaps and compensatory or mitigating controls for those gaps.
- Identify the monitoring use cases that apply to your enterprise's database infrastructure, and deploy tools to support those use cases effectively and efficiently.
- Develop and communicate a clear policy specifying what database-related behaviors should be audited and why.
- Conduct a database risk assessment, applying a balanced approach to risk management and mitigation based on risk, criticality, and regulatory and other compliance requirements.

WHAT YOU NEED TO KNOW

This document was revised on 6 May 2010. For more information, see the Corrections page on gartner.com.

Gartner

Certain types of behavior by organizations and individuals with access to enterprise databases may indicate serious problems that can impact security, privacy, confidentiality and data availability. Security and risk professionals should develop systematic processes for monitoring these behaviors, and implement controls to mitigate the risks associated with them.

ANALYSIS

Context

Gartner has seen a dramatic increase in the number of relational database management systems (RDBMSs), as well as an increase in the sizes of these critical data stores. The misuse of these databases and the information they contain – whether malicious or accidental – presents serious risks for enterprises. Auditors, security and risk professionals, and many other enterprise stakeholders need to monitor behaviors and activities that could be indicators of such abuse.

Analysis

Databases – especially RDBMSs – are growing larger all the time, and the information they hold is increasingly sensitive and subject to compliance requirements of many different kinds. These sensitive data types include intellectual property, personally identifiable information, personal health information and financial information. Auditors (internal and external) are asking who has access to this information and what they are doing with that access; security organizations are being called on to help provide answers. These issues raise serious security and privacy concerns, but they also present risks in other areas, including concerns about system and data availability. These concerns extend well beyond auditors. Other stakeholders, including chief information security officers and other senior-level security and risk professionals, and data and business process owners, need to know much more than they currently do about their enterprises' database activities. For this reason, we have compiled a list of 10 critical database activities and behaviors – segmented by four sets of roles – that enterprises should be auditing now.

Role Type No. 1: Privileged Users

Users with special, high-level privileges – typically database administrators (DBAs), superusers and system administrators – should always be subject to intense scrutiny from the security organization and from auditors. The reason is obvious: These users have visibility into, and access to, data and underlying systems, so they can potentially do enormous damage. They should be subject to rigorous background checks, and should be monitored and audited for four potential problem activities:

- **Access to, deletion of, or changes to data:** Privileged users, with very rare exceptions, do not need access to the actual data they manage (for example, the content of database tables). The potential for abuse is obvious – a DBA could, for example, access the payroll system to learn fellow employees' salaries, or even to change his/her own salary information. A system administrator might also alter financially relevant information, deliberately or inadvertently, causing Sarbanes-Oxley Act violations in the U.S. It is difficult to assess how serious a problem this currently represents, because many enterprises are reluctant to publicly acknowledge such cases; however, anecdotal evidence suggests that privileged-user access is a significant real-world problem. Preventive controls are difficult to implement in this area, but detective controls can be effective in limiting the damage and preserving the audit trail.

- **Access using inappropriate or nonapproved channels:** Accessing databases outside of normal channels can also be symptomatic of compromised accounts being used by external attackers. Best practices call for DBAs to use specific, approved tools – for example, Tool for Application Developers (TOAD) for Oracle databases. In practice, however, DBAs may access databases using applications such as Microsoft Excel, or by connecting directly to the database, which bypasses standard monitoring and tracking capabilities. Another common problem is the privileged user who makes a remote console connection to the database, or simply enters the data center and physically accesses the database, bypassing network- and application-layer controls, concealing problems that security information and event management (SIEM) and monitoring controls might otherwise detect. In addition to the risks associated with accidental or deliberate disclosure of data, these practices also present potential availability and integrity risks.

- **Schema modifications:** The schema – the metadata and the rules applied to the database's structure – is central to its secure and efficient operation and management. Schemas and metadata must be kept absolutely consistent; inappropriate or unauthorized modifications to the schema can be extremely damaging. A DBA could, for example, create a brand-new table, copying the data from another table into the new table, download the new table – which probably would not be audited, because its existence is unknown – and then delete that table. The result – the DBA has accessed the data without triggering monitoring or auditing. Changes to the schema are not necessarily malicious. They may be entirely inadvertent, but even mistakes can seriously impact data availability.

- **Unauthorized addition of user accounts or modification of existing accounts:** A DBA or other privileged user who knows his own activities are audited and logged could create an account in a fictitious name, use a dormant account, or change a valid account to give it higher levels of access. The new or altered account could then be used to access or change data, and then be deleted so that no one knows the inappropriate activity has taken place. The opportunities for large-scale data

breaches and identity theft using this technique are obvious. Further, the complicated, nested role-based permission structures typical of RDBMSs can lead to unintended levels of access that might not be identified in normal operational activities.

Role Type No. 2: End Users

End users – individuals who have legitimate access to data through some type of application – present serious risks for deliberate as well as unwitting misuse of that data. Security professionals should monitor these roles for three potential problem behaviors:

- **Access to excessive amounts of data or data not needed for legitimate work:** Gartner recommends the "least privilege" approach to data access as a best practice, but we recognize that this is difficult to implement. In real-world environments, end users are typically granted more data access than they need to do their jobs. For this reason, enterprises should set thresholds for "typical" levels of data access and trigger investigations on activities beyond those thresholds. For example, a call center employee might access approximately 50 sets of customer financial records in a typical working day. If that same worker suddenly accesses thousands of sets of records, that activity should be taken as a clear warning sign of potentially damaging activity. For the same reason, an end user accessing data that is not required for his/her normal role – for example, a customer service representative downloading HR records for other employees, or a data center employee accessing a celebrity's healthcare information – should trigger an immediate investigation.

- **Access to data outside standard working hours:** Many of the behaviors discussed up to this point relate to insider threats of various kinds, but this is one that also raises the strong possibility of external attack. When a company's normal working hours are Monday to Friday from 9 a.m. to 5 p.m., someone accessing a database on Sunday at 3 a.m. may indicate that an attacker has attempted to gain access using hijacked credentials. Unless monitoring is implemented for reporting on this type of activity, the unauthorized activity is likely to go entirely undetected, until it results in a highly damaging, highly publicized data breach.

- **Access to data through inappropriate or nonapproved channels:** This problem is similar to that for privileged users, but the risk is somewhat different. End users sometimes access data directly, without using the approved applications or channels. They sometimes do this simply for convenience. But the result may be undetected changes to data that seriously impacts availability and data integrity. Enterprises need detective security measures to determine whether end users are trying to bypass proper channels. One possible scenario could take place if an application required creation of local database accounts. Users could potentially go directly to the database, bypass application-level controls, and view or alter critical data.

Role Type No. 3: Developers, System Analysts and System Administrators

These users present two specific types of IT risk. The first is the potential for data breaches that compromise intellectual property or personal privacy, because these roles necessarily have extremely high levels of privilege and access. A much more serious problem, however, is that these technically skilled individuals often have the ability to access or change systems that are in live production, which can result in poor performance, system crashes and, in some cases, security vulnerabilities. This is the primary behavior by individuals in these roles that auditors should watch for:

- **Access to live production systems:** Best practice indicates that developers and other users with similar roles and responsibilities not have access to production systems using privileged accounts. Any access to these systems that is required for normal activities should be via standard user accounts. The reality, however, is that the overhead of using two accounts leads to violation of this policy. There are several risks associated with this – changes made to live systems, especially without testing, could easily result in system instability and crashes. Application or database changes made to live systems could also alter the effective permissions and result in users having access to data to which they should not have access.

Role Type No. 4: IT Operations

The IT operations organization – not only the individual employees, but also the processes for which the organization is responsible – has a significant impact on the proper functioning and management of enterprise databases. Their database-related activities should be audited in two key areas:

- **Unapproved changes to databases or applications that access the database:** IT operations personnel have a strong tendency to want to fix problems as soon as they are recognized, without necessarily planning, testing or evaluating their "fixes" or consulting the appropriate stakeholders. Auditors are continuing to focus on change and configuration management processes, especially within systems containing or processing regulated data. When databases are involved, this can cause serious data security and availability issues. Table structures, data types and other key database elements should not be changed unless the changes are mapped against a change management system of some kind.

- **Out-of-cycle patching of production systems:** Most enterprises with robust operational management processes have defined "operational windows" for patches (for example, applying patches only on certain dates or at certain times). Patches that are applied "on the fly," or otherwise outside normal patch management processes, may adversely impact data storage and availability – and may be a sign of a larger problem.

All 10 of these database-related behaviors should be part of any enterprise's standard auditing regimen. They are not all simple to monitor or control, and some are typically subject only to after-the-fact detective measures. However, all 10 present serious security, privacy, regulatory or operational risks, and auditors, security and risk professionals and other stakeholders cannot afford to ignore them.

Use Cases for Monitoring Tools

Many technologies are available that can help enterprises monitor these 10 behaviors. The key to selecting the appropriate tool is to first identity applicable use cases. Figure 1 can be used in the evaluation and selection process.

Key Facts

Enterprise databases – especially RDBMSs – now contain enormous amounts of critical, highly sensitive information. This information is frequently subject to rigorous legal, regulatory and other compliance requirements, and its misuse, exposure or unavailability could cause serious damage to the enterprise. Certain types of behaviors represent clear indicators of potential database security problems, but few enterprise auditors routinely monitor these behaviors.

Figure 1. Applicable Use Cases for Use in the Evaluation and Selection Process

		DAM	DLP	SIEM	NIDS	DB Scanner	CCM	Fraud	IAM
Privileged Users	Access or changes to data	●	◐	○	○	○	○	◐	○
	Access via inappropriate or unapproved channels	●	◐	●	◐	○	○	◐	○
	Schema modifications	●	○	◐	○	◐	●	○	○
	Addition or modification of accounts	●	○	◐	◐	◐	○	◐	◐
End Users	Access to excessive or unneeded data	●	◐	◐	◐	○	○	●	◐
	Data access outside standard hours	●	●	◐	●	○	○	●	◐
	Access via inappropriate or nonapproved channels	◐	◐	◐	●	○	○	●	◐
Developers Sys. Admins Analysts	Access to live production systems	◐	◐	◐	●	○	○	◐	◐
IT Ops	Nonapproved changes to databases or applications	◐	○	◐	○	●	●	○	○
	Out-of-cycle patching of production systems	◐	○	◐	◐	●	●	○	○

Legend

Database Activity Monitoring	DAM	Database Vulnerability Scanner	DB Scanner
Data Loss Prevention	DLP	Change and Configuration Management	CCM
Security Information and Event Management	SIEM	Fraud Monitoring and Detection	Fraud
Network Intrusion Detection/Prevention	NIDS	Access Management	IAM

Value/Applicability

- ● High
- ◐ Good
- ○ Poor or not applicable

Source: Gartner (April 2010)