Realtime
publishers

The Essentials Series: Role of Database Activity Monitoring in Database Security

Data Discovery and Classification in Database Security

sponsored by

IMPERVA®

by Dan Sullivan

Copyright Statement

Data Discovery and Classification in Database Security

Database security is a highly complex but essential component in today's business environment. Core business operations often depend upon the ability to acquire access to, manage, and preserve growing volumes of data. Relational database management systems from Oracle, Microsoft, IBM, and others provide highly available and highly scalable database applications that enable IT solutions demanded by today's businesses. The same databases that underlie critical applications are also prime targets for cybercriminals, disgruntled employees, and unscrupulous competitors. Maintaining adequate database security is a multifaceted challenge.

This Essential Series will examine the role of database activity monitoring in database security and describe a management framework for establishing and maintaining a database activity monitoring practice in your organization. Each of the articles in this series will address a distinct topic:

- This article, the first of three, discusses the need for database discovery and data classification, two processes that constitute the first steps in database activity monitoring.
- In the second article, we turn our attention to understanding database vulnerabilities, types of data vulnerabilities, and vulnerability assessment scanning.
- In the third article, we build on the processes described in the first two articles to describe how to implement mitigation strategies and ongoing controls, including database activity monitoring.

It should be noted at the outset that successful database security strategies are built on a combination of technologies and management practices. Throughout this series, we will consider best practices for combining both to realize the goal of improved database security; but first we will consider an all-too-common hurdle to database security.

Security Management Silos

Enterprise databases require specialized skills to design, implement, and manage. From installing, configuring, and monitoring to backing up, tuning, and managing storage, what may seem to be common IT operations are actually distinct procedures in database administration. For example, when backing up a database, the backup process must account for the fact that programs may update different blocks of a database file in a single transaction, including a block that has already been backed up. Another example of a common IT operation is maintaining access controls, but once again, databases have distinct requirements, including fine-grained access controls on tables, columns, and even rows of data.

Monitoring database activity is especially challenging because there are many subcomponents, such as database listeners that establish connections to a database, storage management processes that allocate and release disk storage as needed, and query processors that execute commands on the database. These components are also important from a security perspective. Attackers can exploit vulnerabilities in database listeners to gain access to the database. Unusual storage management activity and excessively large I/O requests in queries can be indicative of a malicious operation on the database. DBAs and database application developers have to understand a broad array of database-specific management and security issues; many will understandably not have time to master broader security issues that network administrators and security professionals face. Similarly, it is not reasonable to expect network and systems managers to learn the intricacies of database security. This is a problem.

Divided We Fail

The division of labor in information security creates a risk of security management silos. Organizations often support multiple database platforms each managed by different groups of DBAs who may not work together and because of differences in terminology, may not communicate as well as expected. DBAs may leave issues related to servers, clients, networks, and other non-database security issues to network professionals, and in what is close to the worst-case scenario, are unaware and unconcerned about broader security issues. The best one can hope for in this situation is that the two realms are well managed and they do not interfere with each other. In practice, such is not the case.

Need for Unified Security Management

We no longer have the luxury of two separate security management silos. DBAs need network security professionals and their experience with the fundamentals of security. Many of the principles and practices in information security apply equally well to database security (the principle of least privilege and rotation of duties are two obvious examples). Network managers and security professionals need the specialized knowledge DBAs have when it comes to questions such as "What kind of protocol is required for a database management system?" or "How should we configure a database security gateway?" Both kinds of professionals have the same goals: protecting the confidentiality, integrity, and availability of data and information systems. Executive managers know that government and industry regulations demand compliance with practices that span database and networking domains.

We can merge database and network security practices. DBAs will benefit from the broad experience of security professionals and network and systems administrators will benefit with improved security on what is often one of the choicest targets for attackers.

Starting Point: Discovering Database Servers and Their Contents

Knowing what is on your network is one of the first steps to implementing a security strategy, and both database and network professionals are well served by discovering databases and their contents.

Difficulties with Database Discovery

When we think of databases, we may think of the production systems that run enterprise applications, but they are just the most obvious instances. It is useful to keep in mind two broad categories of database in an enterprise: the formally managed and informally managed.

- Formally managed databases include those created and managed according to IT policy. These include development, test, and production environments that DBAs actively manage and run on servers intended for database systems.
- Informally managed databases are created outside of the normal provisioning process by developers or department staff using hardware available to them. These may be created for short- or long-term efforts and may run "under the radar" of IT management.

IT staff can document the formally managed databases and their contents at any point in time, but keeping that information up to date in a cost-effective manner is a challenge. Changes occur because of mergers and acquisitions, employees leave their positions, new projects are initiated, and old projects are closed. Change management is critical in these environments, but even that cannot address the problems caused by informally managed.

It is important to understand what informal databases are in use and what data is on them. An overzealous developer might decide to bypass normal procedures and speed up a project by creating a database and copying production data into it for testing purposes. The database may not be properly configured, may use default accounts and passwords, may not be sufficiently protected by a gateway device, and may hold customer credit and financial data in violation of privacy regulations. In other words, it is a prime target for an attempted data breach.

We should keep in mind when we perform database discovery that we are likely dealing with heterogeneous environments. As companies grow by acquisition and merger, different database management systems may be introduced. A developer setting up an informal database may decide to use one he is more familiar with even if it not standard for the company. Automated discovery methods should be used to detect multiple types of databases as well as non-standard configurations (for example, database listeners configured to use non-standard ports).

Database Configuration and Contents

For security purposes, we need to discover and inventory databases and in particular, we should collect three types of information about each database:

- Database software and configuration information
- Database contents
- Access information

Database software and configuration information includes the database product name, version, patch level, and optional components installed. The optional component information is useful for determining whether any databases are vulnerable should a security flaw be discovered in an optional component. Operating system (OS) information, including version and patch level, should be collected as well.

The contents of databases should categorized by function and security classification. Functional categories describe the business purpose of data; examples include financial data, customer data, inventory, production controls, and so on. Functional categories are not necessarily exclusive and data may fall into multiple categories. Data should also have a security classification—such as public, sensitive, private, and confidential. In this scheme, public data may be disclosed without harm to the business; sensitive data should not be disclosed but if it were would not cause serious harm to the business, its customers, or other stakeholders; private data is customer data or other data held in trust and protected by regulation; confidential data is business data that, if disclosed, could cause serious harm to the business, such as trade secrets.

The third element of database content information describes access to data. Essentially, we should document who has access to the database and what privileges they have. Privileges should align with organizational responsibilities; for example, we would expect human resources staff to have access to HR data but not inventory control data. Access should be granted through accounts linked to a single individual or application to ensure accurate and complete audit control. Common practices, such as sharing accounts, are driven by informal business processes and should be eliminated when possible. Another situation that creates potential security vulnerabilities is the need to hard code authentication credentials in legacy applications. There may be no better practical solution to shared accounts or hard coded credentials, but all instances should be known and additional mitigating controls should be in place.

Database discovery is the first step to implementing a database activity monitoring strategy. We should remember that the process is likely to uncover informally managed databases, over-privileged accounts, and unauthorized copies of private or confidential data. All these situations should be corrected by putting the database under formal controls, enforcing existing security policies, and compensating for known vulnerabilities that cannot be eliminated.

Summary

Databases are often some of the most complex applications in a business. DBAs, network managers, and security professionals share responsibility for protecting the confidentiality and integrity of data as well as the availability of applications. In the past, a division of labor between databases and the rest of the network made sense because of the specialized skills needed for management of each. The security challenges facing organizations today require a more coordinated security strategy. Database activity monitoring is one security measure that can benefit both database and network security.

The next article will discuss the step that comes after discovery: vulnerability scanning and assessment.