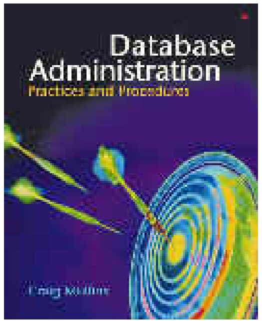
Craig S. Mullins

Return to Home Page

July 2004

DATABASE
TRENDS AND APPLICATIONS



The DBA Corner

by Craig S. Mullins

How Secure Are Your Databases?

Increasingly, security issues are on everyone’s mind these days. We are constantly bombarded with images on the daily news that underscore just how important security is: homeland security, personal security, security in general. Every time you open your e-mail in box vigilance is required to avoid stumbling into some virus trap in one of those hundreds of spam messages. And governmental regulations on corporate governance require more diligent security mechanisms.

With all of the above in mind then, how would you answer the question posed by this column’s title: how secure are your databases? Really take some time to think about it before answering though. I’m not just talking about the basic DBMS-based granting and revoking of privileges.

First of all, do you even know what is being done to your data and who is doing it? Being able to answer this question requires the implementation of auditing and database usage reporting. Typically, audit reports show things like a history of changes made to database privileges, changes to database structures, changes to data, and access to data. To be useful, the report should minimally show the database, table, user, type of change/access, and timestamp. Even more useful would be a before and after image of any change. Some DBMS products provide native capabilities for auditing data access and modification, but turning on these features can increase overhead thereby degrading database performance. Even so, in this day and age you may need to bite the bullet and enable auditing. Of course, some third party products are available that mine this information from the database log files – an attractive option for avoiding the performance hit of audit traces.

Another consideration for database security is the ability to monitor and report on user behavior. Many studies have shown that internal users are a bigger threat to security than external hackers. So you better do your best to protect your databases from damage done by disgruntled employees or fired employees whose access has not been terminated. This is a challenge. One approach is to maintain a baseline of standard user behavior and report on anomalies. For example, consider a user whose regular pattern is to access tables A, G, T, and Z weekdays from 9 to 11:30, is logged off until 1:15, and then is back on the system again until 5:30 accessing the same tables, plus another table from 3:00 to 3:30. Wouldn't it be interesting to be able to report on deviations from that norm? A report that showed the user was in on Saturday accessing table T would be useful if data corruption appears in table T on Monday. Similarly, it would be useful to note if the user did not access the 3:00 table as he normally does.

And how prepared are you for vulnerability management? In other words, are you sure that your environment is perfectly set up and secured? Periodic scanning for potential vulnerabilities is a prudent approach to take. For example, a regularly scheduled report showing DBMS patches not applied, default passwords that were not changed, and the like can help to avoid potential security violations. To be successful, database vulnerability management should be approached like PC virus scans. A regularly updated database of vulnerabilities for each DBMS should be available and organizations should be able to register software that checks their systems against known problems. What DBA group wouldn't want to subscribe to that service?

Of course, this article just scrapes the surface of database security. We haven’t even talked about SQL injection attacks and integrating database security with operating system security. Indeed, there is a lot to think about – and a lot to do. But failing to properly secure your databases is just asking for trouble.

To conclude, every DBA-in-waiting would do well to take every opportunity available to learn about database management systems, database administration, and IT in general. Reading the latest information in industry journals and books, attending and participating in local user groups, and sharing your experiences with others are all good techniques to add to your database knowledge – and therefore, are useful tactics to deploy in your quest to become a DBA.

From Database Trends and Applications, July 2004.

Home.