**Threats to Database Security**

With the increase in usage of databases, the frequency of attacks against those databases has also increased. Here we look at some of the threats that database administrators actually can do something about.

* + - Database attacks are an increasing trend these days. What is the reason behind database attacks? One reason is the increase in access to data stored in databases. When the data is been accessed by many people, the chances of data theft increases. In the past, database attacks were prevalent, but were less in number as hackers hacked the network more to show it was possible to hack and not to sell proprietary information. Another reason for database attacks is to gain money selling sensitive information, which includes credit card numbers, Social Security Numbers, etc. We previously [defined database security](http://www.brighthub.com/computing/smb-security/articles/61400.aspx) and talked about [common database security concepts](http://www.brighthub.com/computing/smb-security/articles/61402.aspx). Now let's look at the various types of threats that affect database security.
    - ***Types of threats to database security***

**1. *Privilege abuse:*** When database users are provided with privileges that exceeds their day-to-day job requirement, these privileges may be abused intentionally or unintentionally.

Take, for instance, a database administrator in a financial institution. What will happen if he turns off audit trails or create bogus accounts? He will be able to transfer money from one account to another thereby abusing the excessive privilege intentionally.

Having seen how privilege can be abused intentionally, let us see how privilege can be abused unintentionally. A company is providing a “work from home” option to its employees and the employee takes a backup of sensitive data to work on from his home. This not only violates the security policies of the organization, but also may result in data security breach if the system at home is compromised.

***2. Operating System vulnerabilities*:** Vulnerabilities in underlying operating systems like Windows, UNIX, Linux, etc., and the services that are related to the databases could lead to unauthorized access. This may lead to a Denial of Service (DoS) attack. This could be prevented by updating the operating system related security patches as and when they become available.

***3. Database rootkits:*** A database rootkit is a program or a procedure that is hidden inside the database and that provides administrator-level privileges to gain access to the data in the database. These rootkits may even turn off alerts triggered by Intrusion Prevention Systems (IPS). It is possible to install a rootkit only after compromising the underlying operating system. This can be avoided by periodical audit trails, else the presence of the database rootkit may go undetected.

***4. Weak authentication*:** Weak authentication models allow attackers to employ strategies such as social engineering and brute force to obtain database login credentials and assume the identity of legitimate database users.

***5. Weak audit trails:*** A weak audit logging mechanism in a database server represents a critical risk to an organization especially in retail, financial, healthcare, and other industries with stringent regulatory compliance. Regulations such as PCI, SOX, and HIPAA demand extensive logging of actions to reproduce an event at a later point of time in case of an incident. Logging of sensitive or unusual transactions happening in a database must be done in an automated manner for resolving incidents. Audit trails act as the last line of database defense. Audit trails can detect the existence of a violation that could help trace back the violation to a particular point of time and a particular user.

**UNDERSTANDING DATABASE SECURITY**

An ever increasing number of databases are needed in business, and, with the advent of the Internet, threats or risks to these databases are increasing apace. In this series, we provide a definition of database security, and look at security concepts and the types of threats involved.

* + - [**Database Security**](http://www.brighthub.com/computing/smb-security/articles/61400.aspx)
    - [**Concepts of Database Security**](http://www.brighthub.com/computing/smb-security/articles/61402.aspx)
    - [**Threats to Database Security**](http://www.brighthub.com/computing/smb-security/articles/61554.aspx)