Security Breach Of A Database

Posted on January 23, 2020

Explanation Of The Tools That Are Available To Database Administers To Prevent Security Breaches

Database security tools are essential components of overall database security. They come in handy in many situations to avert security attacks, breaches, and threats to an extent and protect the safety of vital data on the computer network. In the following, there are descriptions of certain tools that can protect the database from any form of a hacking attack.

MSSQL DataMask

Any organization can make the mistake of using production data as test databases for different experiments. To avoid this, MSSQL is a tool that provides IT professionals with the ability to mask data for any testing purpose, such as development or outsourcing projects that involve databases from SQL servers. Unmasked production data that is used for any testing purpose has a severe threat of a security breach, such as getting stolen or being contaminated. MSSQL allows data to be masked that can be categorized as personally identifiable, personally sensitive, or commercially sensitive.

Scuba

This is a free database security tool from Imperva. This is a very handy security tool that can scan and analyze more than 2000 problems in a network with a sensitive database. These problems can be weak passwords, missing patches, or known configuration risks. Scuba is popularly being used over enterprise networks as a database patch-up enhancer. It is noticeable that missing patches on a database or any other server create an opportunity for hackers to break into network systems.

AppDetectivePro

It is software that scans databases and big data stores and, as a result, immediately identifies configuration problems and issues with access control, absent patches or a toxic combination of settings that can appear in the form of certain common security attacks by hackers such as escalation of privileges or denial of services attacks, data leakage and unauthorized alteration of data (“Top 10 Database Security Tools You Should Know”, 2017).

Strategies Available To Database Administrators That Would Prevent Security Breaches

It is important to come up with robust strategies to protect the data in database systems to ensure the proper workflow of organizational affairs in a secure and effective manner.

Strategy#1. Good practice includes database and data host server security hardening and proper patching, but along with this step, proper vetting of database administrators and effective user management is also necessary to mitigate security threats ("Database administration security strategy," 2017).

Strategy#2. Never allow excessive default database privileges that exceed the job description or job requirements. As an example, a banking worker with a job that requires altering only the account bearer's contact information in the database can abuse his or her privileges to add to the balance of the colleague's saving account. Moreover, many organizations ignore updating the access rights of employees who are promoted or demoted on a job role in an organization or leave altogether, leaving a loophole in the body for a breach. These account updates and audit issues should be strictly dealt with.

Stretegy#3. Take strict measures against SQL injection and NoSQL injection attacks. Since SuperMart is moving ahead to acquire a data warehouse, they will be dealing with big data, and the SQL databases may be upgradeable to NoSQL. In both cases, when you have a SQL database or a NoSQL database, have the best technology in place to safeguard against this highly common form of database attack.

Strategy#4. Always keep the anti-malware technology updated to have a sufficient safeguard against malware infection of the database of the organization and have regularly automated and manual scan and measure the level and the risk of infection of the network ("Top Database Security Threats and How to Mitigate Them," 2017).

Identification Of Laws, Rules, And Standards That May Apply To Retail Chain (Like SuperMart) Security Breach

In the following, certain laws, rules, and standards can be implemented for SuperMart security breaches.

Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is a set of rules that ensures the security of customer account data information when making the payment of goods at retail

stores. The important bodies that get affected include retailers like SuperMart.

Electronic Fund Transfer Act, Regulation E. Enacted in 1978, this law protects the rights of consumers who engage in electronic fund transfers from errors and fraud. This law encompasses Point of Sale (POS) security also which many retail stores like SuperMart utilize. Other ways of fund transfer may also include transactions made on the internet, where most security breach attacks originate.

Fair and Accurate Credit Transaction Act (FACTA), including Red Flags, Rule. It helps consumers of retail stores and other online markets from identity theft. This law also facilitates the accuracy and privacy of information, and in a data breach, a hacker may steal this information and misuse it (Staff, 2017).

References

Top 10 Database Security Tools You Should Know. (2017). *InfoSec Resources*. Retrieved 27 July 2017, from https://resources.infosecinstitute.com/top-10-database-security-tools-know/#gref

Database administration security strategy. (2017). *ComputerWeekly*. Retrieved 27 July 2017, from https://www.computerweekly.com/opinion/Database-administration-security-strategy

Top Database Security Threats and How to Mitigate Them. (2017). *SHRM*. Retrieved 27 July 2017, from https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx

Staff, C. (2017). *The security laws, regulations and guidelines directory*. *CSO Online*. Retrieved 27 July 2017, from https://www.csoonline.com/article/2126072/compliance/compliance-the-security-laws-regulations-and-guidelines-directory.html

