Top-10 guide for protecting sensitive data from malicious insiders

By Brian Contos, Chief Security Strategist, Imperva

This guide explores the top ten ways of protecting sensitive data from the very people who need access to it. While this is a difficult problem to address, it is not impossible – especially when leveraging the right tools.

1 – To secure it you have to know about It

Organisations may not know where sensitive information is in order to protect it. Once the databases and related data stores have been identified, it's vital to classify the sensitive data and identify the objects contained.

2 – Don't trust native database tools

If a malicious insider has access to the database and can possibly manipulate the native database audit logs, then these logs are useless. Capturing database audit logs should be done independently of the database tools, thus enforcing separation of duties.

3 – Monitoring the good and the privileged

Insider threat is more about detection than prevention. That means monitoring how users are interacting with your sensitive data.

The Good: because the term 'insider' implies a certain level of trust and access beyond that of an outsider.

The Privileged: privileged users are a subset of the insider and have the ability to cause more damage, more quickly, and more easily than any other group; they should not be responsible for monitoring themselves.

4 – Profiling isn't just for the FBI any more

It is important to profile application and database interactions. This enables better protection against simple attacks like SQL injections and helps identify more subtle attacks such as those that target business logic flaws.

5 – You can't arrest an IP address

The reconciliation of Web application and database activity should be done outside of the Web application and database and be independent of vendor, version, etc. Tracking user sessions in this way allows for greater control of session tracking without putting additional resource strain on the Web and database applications themselves.

6 – Augmenting machine-based analytics with human intuition

Because IT security may not have the 'big picture' for every person in every organisation, it's important for the reports to be reviewed by various stakeholders such as non-technical managers, HR, and legal. This combination of real world analysis supported by detailed application and database evidence can yield more accurate results.

7 –Forensic crime scene investigation through audit logs

In most insider threat investigations, once signs of malicious activity are identified, three questions are asked: what else has the insider done, how long has this been going on, and who else might be involved in similar activities. Leveraging visual analytics to investigate attacks can result in flagging malicious activity in minutes.

8 – Sensitive data resides in databases

Two solutions that work well for the needs of DBAs and IT security are Database Firewalls (DBFW) and Database Activity Monitoring (DAM) solutions. Together these provide a combined solution for database protection, monitoring, and auditing that is completely independent from users.

9 – Users get to databases through web applications

While sensitive data resides within the database, most users access that database through a Web application. Many organisations use a Web Application Firewall (WAF), modern WAFs are able to protect against technical attacks, business logic attacks, and provide a number of correlation, profiling, and adaptive capabilities needed to address today's complex attacks.

10 –Needles hiding in stacks of needles

Insider threat analysis benefits from multiple sources of data-centric information because a single source might not provide the complete story. Discovery and classification should be used to identify critical assets and the information they contain. WAFs should be leveraged to protect applications, DBFWs to protect databases, and DAMs to provide database auditing. Together these solutions can be brought together to provide insider threat mitigation for even the most complex, distributed, and mission-critical environments.

About Imperva

Imperva, the Data Security leader, enables a complete security lifecycle for business databases and the applications that use them. Over 4,500 of the world's leading enterprises, government organisations, and managed service providers rely on Imperva to prevent sensitive data theft, protect against data breaches, secure applications, and ensure data confidentiality. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring from the database to the accountable application user and is recognized for its overall ease of management and deployment. For more information, visit www.imperva.com.

Media queries
Grenadine Lau
Imperva
Phone: +65.6749 4482
Mobile: +65.9666 1886
Email: Grenadine.Lau@Imperva.com
David Frost
PR Deadlines Pty Ltd, for Imperva
Phone: +61.2.4341 5021
Mobile: +61 (0) 408 408 210
Email: davidf@prdeadlines.com.au