White Paper

Security Trends

Facing Reality: Top Database Security Trends

Database security continues to be a top priority

Detecting and stopping a data breach has always been a challenge. However, recent regulations, which require organizations to notify the public of a data breach that involves consumer data, have heightened the need for effective database security tools. According to the Verizon '2010 Data Breach Investigations Report', 92% of the breaches that compromised data involved corporate databases.

Forrester analyst, Noel Yuhanna, states in the 2011 Forrester Wave report on DAM vendors, "It takes a hacker less than 20 seconds to execute a query and retrieve sensitive information once he has broken into an application or database. Because it is not possible for a human to detect such attacks, the need for real-time database security solutions has become critical."

Enterprise database infrastructure is subject to an overwhelming range of threats. Securing databases and the data they host is challenging not only because of the volume of data spread across heterogeneous platforms, but also because of the increased sophistication and rising rate of database security threats.

This paper reviews the top database security trends that IT managers and security teams struggle to keep up with, including:

- Advanced Persistent Threat (APT)
- SQL Injection Attacks
- Implementation of Audit Controls
- Database Patch and Configuration Management
- Limiting Users Rights to Data, Based on Business Need-to-Know
- Abuse of Legitimate Data Access Privileges
- Data Security in the Cloud

> *"The need for real-time database security solutions has become critical."*

Advanced Persistent Threat

Security researchers have discussed advanced persistent threats (APTs) for some time. Recently, we have seen a steep increase in the number of organizations hit by this type of attack. We have also seen the threat spread beyond government agencies to target enterprise companies. These breaches confirm that APT is not confined to a specific type of organization or sector.

APTs are built to circumvent existing perimeter and endpoint defenses. They typically leverage social engineering and human curiosity to spread malware. Hackers search for publicly available information about target companies and key employees, and then send the employees a message that appears to be from a friendly source, such as a coworker, friend, or family member. The message is crafted to trick the employee into letting his/her guard down (a technique often called Spear Phishing). The message asks the employee to log into a Web site that requests the employee to input his/her username and password, or click a link that will download malware. If a single employee falls for this scam the attacker can gain further access into the target company's resources.

APTs do not "defeat" security products; they find ways to fly below the radar of existing technology. It is difficult to prevent APTs and the spread of malware. In most cases, employees are not aware their computers have been infected or their accounts have been compromised. Therefore, the attacker uses the compromised computers and accounts to get into the network and possibly install a remote administration tool that enables control of the compromised machines.

In order to protect corporate resources and prevent a data breach, it is necessary to continuously monitor activity related to corporate resources, including databases, which are both critical for operations and contain sensitive data. Advanced profiling technology should be used to learn the behavior of users and applications, and identify abnormal behaviors that do not match the "normal" behavior profile. These "abnormal" activities may indicate malicious activity.

Imperva SecureSphere delivers automated, scalable database activity monitoring, auditing, and reporting. Imperva's Dynamic Profiling automatically profiles application and database elements, and builds a baseline of acceptable user behavior. By building an accurate profile, or "white list" of application and database usage, Dynamic Profiling enables SecureSphere to identify abnormal activities.

SQL Injection: Exploiting Application Vulnerabilities that Target Databases

Over a decade has passed since we witnessed the first SQL injection attacks. This type of attack continues to be one of the most predominant application and database threats. Recently, there has been a rapid spread of the LizaMoon virus through SQL injection attacks. Hackers injected SQL commands into the associated databases of Web sites by exploiting weaknesses in Web applications. The LizaMoon code was designed to redirect users to different fake Web sites where they were then asked to download malware.

SQL injection attacks take advantage of non-validated input vulnerabilities to pass SQL commands for execution by a back-end database. Most SQL injection attacks are executed through an application that accepts user-supplied input for query parameters. Another type of attack, one that is less prevalent in real-world scenarios but can cause major damage to an organization if it succeeds, is a direct database SQL injection attack through database stored procedures.

Today's SQL injection attacks are sophisticated and constantly evolving; changing in shape and who they target. Many organizations use vulnerability scanning technologies to scan applications and databases, identify vulnerabilities, and remediate the weakness. Since development and deployment of appropriate patches can take months, virtual patches are often used to provide immediate protection. Virtual patching is a firewall rule that blocks attempts to exploit vulnerabilities. By applying a virtual patch, you can quickly mitigate the risk of a SQL injection attack without changing the vulnerable application code.

Two solutions should be considered for virtual patching and effective, real-time SQL injection protection:

- **A Web Application Firewall (WAF)** provides Web-level protection against exploitation of both known and unknown Web application vulnerabilities.
- **A Database Firewall (DBF)** provides a virtual patching solution for databases, including direct SQL injection attacks that exploit vulnerable functions and stored procedures. This solution also identifies suspect database activities and abnormal behaviors that indicate an attack.

Imperva SecureSphere Data Security Suite provides an integrated WAF and DBF solution. Combining the advanced capabilities of the market-leading Imperva WAF and DBF solutions, SecureSphere Data Security Suite provides the most complete protection against SQL injection.

Implementation of Audit Controls

Auditing database activity is critical to organizations not only to satisfy regulatory compliance requirements, but also to help control and reduce risk to business operations that rely on corporate databases. Business owners, IT security, and database administrators need visibility to ensure proper database operations. This includes tracking administrative activities, data changes, and data access. Forensic investigations often require information regarding database events and some context about the users, the source application, and the results of the event. In the case of a data breach, detailed, real-time alerts and audit analysis tools can reduce the impact of the breach by improving response time and enabling efficient damage control.

In order to bolster security, support operations, and meet compliance requirements, more organizations are looking to implement or extend existing deployments of database activity auditing. However, many organizations struggle with the technical aspects of database auditing as well as the amount of funds and resources it requires.

To ensure cost-effective database auditing, organizations should consider the following:

- **Monitor Impact on Database Servers:** Most database activity monitoring (DAM) solutions monitor database activity using agents or by collecting various database logs. While monitoring on the server is required for capturing privileged operations performed directly on the server, it is important to consider the overhead caused by this method. Turning on the native audit utility, for example, can cause significant performance degradation due to its resource consumption.

Imperva offers light database agents designed to audit database activity with minimal overhead. Imperva also offers network monitoring appliances that have zero impact on database activity. The SecureSphere agents and appliances can be combined in a hybrid mode to optimize the DAM deployment.

- **Audit Visibility and Details:** Not all DAM solutions provide the same visibility. Those that audit only SQL activity, for example, miss administrative activity that is not executed as SQL commands, such as some export commands.

Unique to the industry, Imperva SecureSphere monitors both the SQL activity and the protocol commands to provide a complete audit trail of database activities. SecureSphere also provides many details needed for understanding the context of the activity.

- **Real-Time Alerts and Analysis:** Real-time alerts allow security teams and database administrators to quickly respond to a database security event and reduce the impact of a breach. Real-time analysis with drill down capabilities supports intelligent decision making.

Imperva SecureSphere real-time alerts reduce mean-time-to-resolution by providing details about the event, including the date and time, SQL activity, source application, number of rows affected, and more. Interactive, audit analytic views enable quick and easy access to audit data without the need to define and run reports.

» **Centralized Management:** In large, for distributed environments, which include heterogeneous platforms, centralized management reduces the amount of funds and resources required for set-up, configuration, and on-going maintenance.

To simplify the management and maintenance of the solution, Imperva SecureSphere's user interface enables central management for audit and security policies, reports, and alerts as well as solution components, such as agents, gateway appliances, storage, and more.

» **Coverage for Heterogeneous Database Platforms:** The ability to provide the same audit controls for heterogeneous databases simplifies policy definition, reporting, and data analysis.

Imperva SecureSphere provides comprehensive coverage for all major database platforms, including Oracle, MS-SQL server, DB2 (LUW, z/OS and DB/400), Sybase, Informix, MySQL, Teradata, Netezza, and Progress.

» **Preserved Integrity of the Audit Trail:** The audit trail should provide a true representation of database activity. Database administrators should not have the ability to turn on/off the audit solution or change audit policies to conceal malicious activity. In addition, no one should have the ability to alter the data in the audit trail.

Imperva SecureSphere delivers automated, scalable activity monitoring, auditing, and reporting for heterogeneous database environments. SecureSphere provides a cost-effective solution for addressing compliance requirements and controlling risk to databases and the business operations that rely on them.

Database Patch and Configuration Management

Even though the importance of patching has been discussed at length, the exploitation of known, patchable database vulnerabilities still exists. While this is becoming less of a trend, the Verizon Data Breach report still reports attacks that exploit older vulnerabilities. These vulnerabilities could have been mitigated with a reasonable patch management cycle.

For example, the SQLslammer worm, which first surfaced in January 2003, exploited a known buffer overflow vulnerability in SQL Server 2000. Microsoft released a patch to mitigate this vulnerability in 2002. Not only was there a large number of unpatched systems that enabled the rapid spread of this worm in 2003, but the worm was still active in 2010. How is this possible? The reality is simple; there are still many unpatched databases.

According to the '2010 IOUG Data Security Survey,' many organizations are not applying critical patches in a timely fashion, which increases their risk of a data breach. Typically, it takes 6-9 months to deploy a patch due to the thorough testing and change management procedures required before a patch can be deployed on a production system. In some cases, a patch cannot be deployed because it creates problems that affect the stability and/or availability of the system.

In addition, some IT managers feel their data is not at risk because their databases are not directly connected to the Internet. This is a false sense of security, as these databases are still accessed by other systems and users, and can be infected with malware that exploit known vulnerabilities. A hacker that has penetrated the network and compromised an existing user account can attempt to exploit these known vulnerabilities.

To mitigate the risk of a database breach, organizations need to establish a continuous vulnerability management program. A vulnerability management lifecycle should include the following steps: vulnerability identification, classification, remediation, and mitigation. To implement effective, repeatable vulnerability management practices across corporate databases, organizations need to automate as many steps as possible.

DatabaseFileWeb

If a database is found vulnerable, the relevant patch should be applied to close the vulnerability. If a database cannot be patched, a virtual patching solution can, and should, be used to protect the database against exploit attempts.

Imperva SecureSphere delivers a vulnerability management solution that audits configurations of corporate databases, scans for known vulnerabilities, and manages mitigation efforts to close security gaps. Virtual patching is delivered by SecureSphere Database Firewall, which provides firewall rules to block attempts to exploit discovered vulnerabilities.

Limiting Users Rights to Data, Based on Business Need-to-Know

Awareness of data breach incidents performed by the "Insider" continues to grow, as does the number of incident reports where data theft and security breaches are tied to employees and contractors. In the U.S., enforcement of legislation, such as the California Data Privacy Act (SB 1386) and Massachusetts Data Privacy Law (Mass 201 CMR 17), drove a steep increase in the number of reported data leakage incidents and, as a result, a constant stream of apologetic letters to customers. Many European states now impose strict fines on companies that do not adhere to privacy laws, which require the publication of all data breaches affecting individuals.

The "Insider" breach is caused by employees or contractors with malicious intent. In some cases, the breach is accidental, but in many cases these incidents are caused by employees who can access data they are not supposed to access. These employees have excessive access rights, a scenario that indicates a user rights management problem.

Many organizations manage user data access rights using mostly manual processes. These processes, like many other manual processes, are time consuming and error-prone. Often, the individuals in charge of these processes do not have clear visibility into current rights, making it difficult or even impossible to validate requests to change or add access rights. These individuals avoid revocation of what might seem to be excessive rights because they do not have a way to validate and determine if the rights are needed or not. In addition, these individuals do not know if the user in question requires the right based on 'business need-to-know.'

As a result, various regulations now require periodic reviews of user rights:

- PCI DSS Section 7 requires organizations to limit user access to the least necessary to perform job functions.
- COBIT Objective DS 5.4 requires user account management and regular management review of accounts and related privileges.
- HIPAA requires covered entities to restrict user access to ePHI based on need-to-know, and tightly control user access rights.
- ISO-17799 objective 9.2.4 requires periodic reviews of user rights and privileges.

Implementation of periodic user rights review processes necessitates the need to have an automated, repeatable way to generate consolidated reports that document current user rights across database platforms. When this information is aggregated through manual processes not only is it time consuming, but by the time the report is generated it no longer reflects the current state.

Imperva User Rights Management for Databases (URM-D) enables organizations to implement a repeatable process for reviewing user rights through automated aggregation of user rights across database platforms, reporting, and analysis of user rights. URM-D helps organizations identify excessive user rights that should be revoked.

Abuse of Legitimate Data Access Privileges

As data breach incidents caused by "Insiders" continue to soar, it's important to note the many cases caused by users who abuse legitimate data access privileges for unauthorized purposes. For example, an employee may have access to certain data for job-related activities, but he/she abuses the data access privilege to perform other activities not related to his/her job.

One of the most publicized privilege abuse incidents occurred during the 2008 election, when an employee of Ohio's Department of Job and Family Services used state computers to search for information on Joe Wurzelbacher (a.k.a. 'Joe the Plumber'). The searches were reported and the investigation concluded that the searches were improper. In response, Ohio legislature enacted ORC 1347.15, which mandates civil and criminal penalties for improper access of personal information within databases.

In another incident, HSBC IT Specialist, Herve Falciani, tried to sell the records of Swiss Bank accounts held by French customers to officials in France, presumably for the purpose of tracking down French residents hiding assets in the private foreign bank. The French authorities notified HSBC of a potential data breach. Approximately 24,000 accounts were compromised.

To prevent privilege abuse, organizations need a solution that enables them to enforce granular access controls and allows users to perform daily job-related activities, yet prevents unnecessary exposure of sensitive data. Effective database access policies must go beyond the basic read/write privileges and consider the context of the activity by taking into account parameters, such as the client application, time of day, location, etc. For example, organizations may need to implement a rule that allows a user to view one record at a time, but does not allow a user to fetch multiple records. Organizations may also need to implement a rule that allows user access to certain information through an enterprise application, like PeopleSoft, but does not allow user access using the ODBC connector of an Excel spreadsheet.

Imperva's advanced profiling technology, which takes into account the context of the activity, is extremely useful in these particular situations. This sophisticated technology automatically creates a model of the context surrounding normal database interactions. SecureSphere Database Activity Monitoring (DAM) uses the generated profile to compare data access requests and identify abnormal activities.

Data Security in the Cloud

In the past couple of years, the use of cloud technologies has increased. Cloud technologies create additional challenges with respect to data and application security. For example, cloud applications, such as SFDC.com, Gmail, MS BPOS, and SuccessFactors, challenge their operators to maintain complete separation between datasets of different customers. Cloud technologies also challenge providers and customers with respect to protecting data from the prying eyes of service administrators.

Cloud	Challenge
Private clouds (clustered servers running virtual machines)	Hard to monitor the communication path to the application because the same application or database server operates from a different physical server at different points in time.
Public clouds (hosting providers)	Challenge operators to maintain partitions between applications and datasets of different users, and at the same time manage application and data security for a large multitude of different applications.
Self-service clouds (aka "platform as a service" or "infrastructure as a service" such as Amazon EC2 or MS Azzure)	Challenge users with a new virtual platform and the need to protect data from cloud administrators.

Considering the different types of cloud forms (private and public, SaaS, PaaS, and IaaS), a set of challenges exists for both providers and consumers. These challenges can be summarized as follows:

- Maintaining partitions between datasets of different customers
- Providing different levels of data security to applications sharing the same logical or physical platforms
- Protecting customer data from the prying eyes of cloud administrators
- Providing solutions that operate over a specialized infrastructure (VM, Amazon AMI)
- Managing application and data security for a large number of applications inside the cloud

Today, security and cloud providers struggle to solve the conundrum of data security in the cloud. Security vendors provide solutions that operate over virtual platforms (VMWare, Amazon), and cloud operators need security solutions that scale and manage security policies on shared platforms, prevent users from accessing data that is not their own, and keep service administrators away from the data they manage.

Conclusion

Today's organizations face increasing pressure to protect and secure corporate databases, and the sensitive data they host. Yet the overwhelming range of threats and technical considerations, make the implementation of effective security controls a challenge. To effectively accomplish database security, organizations should invest in a database activity monitoring technology that monitors database activity and data access, identifies (optionally blocks) attacks and unauthorized access, enables effective user rights management and removal of excessive user rights to data, and supports risk mitigation processes through patching and vulnerability assessments.

Imperva SecureSphere Data Security Suite is the market-leading data security and compliance solution. SecureSphere protects sensitive data from hackers and malicious insiders, provides a fast and cost-effective route to regulatory compliance, and establishes a repeatable process for data risk management.

About Imperva

Imperva is the global leader in data security. Our customers include leading enterprises, government organizations, and managed service providers who rely on Imperva to prevent sensitive data theft by hackers and insiders. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring for databases, Web applications, and file systems.

To learn more about Imperva's solution visit www.imperva.com.

Imperva
Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com

© Copyright 2011, Imperva
All rights reserved. Imperva, SecureSphere, and "Protecting the Data That Drives Business" are registered trademarks of Imperva.
All other brand or product names are trademarks or registered trademarks of their respective holders. #WP-DATABASE-SECURITY-TRENDS-0611rev1