InformationWeek
:: analytics
Analytics.InformationWeek.com

January 2011
$99

Strategy Session

Presented in conjunction with

SECURITY dark READING
Protect The Business Enable Access

DB2 Gets Safer ... Finally

IBM Makes Security a Priority

Security has not been a priority for DB2 users, and for years, IBM lagged behind the rest of the industry when it came to protection features. But a realization that DB2 is increasingly vulnerable to threats has spurred something of a transformation. In this Tech Center report, we explain why DB2 users need to focus on security, and how to meet essential vulnerability assessment and remediation, monitoring and audit requirements using tools in the IBM portfolio.

By Adrian Lane

Report ID: S2390111

TABLE OF CONTENTS

4 Author's Bio

5 Executive Summary

6 What Makes DB2 Security Different?

7 The Evolution of DB2 Security

- 7 *Exposure to Threats*
- 7 *From General to Targeted Attacks*
- 8 *Focus on the Insider*

9 Security Technologies

- 9 *Native DB2 Tools*
- 10 *Data and Database Discovery*
- 11 *Monitoring and Blocking*
- 13 *Database Assessment*
- 15 *Patch Management*
- 16 *Auditing*

19 Related Reports

ABOUT US | ***InformationWeek Analytics'*** experienced analysts arm business technology decision-makers with real-world perspective based on a combination of qualitative and quantitative research, business and technology assessment and planning tools, and technology adoption best practices gleaned from experience.

If you'd like to contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com,* executive editor **Lorna Garey** at *lgarey@techweb.com* and research managing editor **Heather Vallis** at *hvallis@techweb.com*. Find all of our reports at *www.analytics.informationweek.com.*

© 2011 InformationWeek, Reproduction Prohibited

TABLE OF CONTENTS

10 Figure 1: Database and Data Discovery

12 Figure 2: How Database Monitoring Works: Basic Collection Techniques

14 Figure 3: Blocking Unauthorized Database Queries

16 Figure 4: Database Assessment and Patch Management

17 Figure 5: How Database Auditing Counters the Insider Threat

© 2011 InformationWeek, Reproduction Prohibited

Adrian Lane
Securosis

Adrian Lane, CTO and analyst at Securosis, has more than 22 years of industry experience, much of it at the executive level. Adrian specializes in database data security and software development. He has vendor experience at Ingres, Oracle and Unisys, and as the CTO/VP at companies such as IPLocks, Touchpoint and Transactor/Brodia. He also brings a pragmatic perspective to selecting and deploying technologies, having worked as CIO in the finance vertical. Adrian presents at dozens of security conferences and writes for several security publications.

© 2011 InformationWeek, Reproduction Prohibited

Executive Summary

There's been a significant shift in DB2 deployments—which now include public-facing applications, virtualization and cloud-based implementations—and with it has come increased exposure to attack. IBM's response has been to close the holes with new technologies: activity monitoring, blocking, data discovery, comprehensive auditing. Yet most DB2 administrators are unfamiliar with the new security tools—attack detection, real-time analysis and automated remediation technologies are geared to data security, but they're overkill for compliance, which has been DB2 admins' more pressing concern.

With its acquisitions of BigFix and Guardium, as well as internal product enhancements, IBM has revamped DB2 security to include features such as:

- Automation of compliance tasks
- Capability of nondatabase administrators to audit database activity
- Ability to block Web-based attacks
- Options to push capabilities beyond compliance "checkboxes"

Compliance remains the principle driver for most database security reviews, so investment in technologies that automate common regulatory processes is understandable. All the tools we discuss in this report automate otherwise manual tasks, and produce reports needed to satisfy external audits. Further, most are simple enough for nondatabase professionals to use, providing separation of duties and minimizing added burden on database administrators.

But make no mistake: The shift in enterprise DB2 usage is about security. New deployment and service models remove supporting infrastructure that isolated the database from certain kinds of attack. The quiet elimination of network restrictions and availability of client-facing applications means DB2 is now subject to the same exposure as every other database platform.

As you leverage your existing DB2 investment to serve new business needs, it will help to understand IBM's security changes and features. This report provides the information and perspective you need.

© 2011 InformationWeek, Reproduction Prohibited

What Makes DB2 Security Different?

The evolution of DB2, and the security threats to both the database and its underlying platforms, have led DB2 administrators down a different path from their Oracle, Microsoft, MySQL and Sybase counterparts. Threats to the DB2 platform and, correspondingly, customer demand for security features, have been slow to emerge. While competitors have scrambled to address vulnerabilities and add security and compliance features, IBM has been slower to implement database security.

Over the past 10 years, IBM has produced only a few new DB2 security features. Highlights of the past decade include labeling—a well designed if not widely used tool to control data access—and table-based encryption to secure data at rest. Other in-house development efforts, such as Audit Management Expert (AME), were well intended additions, but failed to meet the performance and ease-of-use expectations of database administrators (DBAs), and so remain on the shelf.

Contrast this with Microsoft SQL Server and Oracle databases, which have seen a steady progression of security features. In 2003, the SQL Slammer worm ran rampant, bringing down thousands of SQL Server databases in a matter of hours. Shortly thereafter, IT professionals became intimately familiar with the term "Patch Tuesday," as they were forced to adopt patch management processes. Within months, Oracle DBA's also learned the hard way about SQL injection, denial of service, code injection and drive-by malware. Oracle and Microsoft were raked over the coals publicly for security flaws that resulted in massive data breaches, while administrators feared their databases would be attacked.

Database vendors such as Microsoft and Oracle responded with assessment tools, modified access controls, network encryption, label security, transparent database encryption, enhanced auditing, deprecated features, tuning guidelines, monitoring and separation of roles years before corresponding features became available from IBM. So why has IBM had the luxury of biding its time when it comes to security? How has DB2 remained largely unaffected as Web-based threats have emerged, managing to duck the headlines during this evolutionary period of database security? Was DB2 more secure than other databases? If these features were unneeded a few years ago, are they really needed now?

We'll answer these questions, exploring how changes in the way enterprises use DB2 expose both the database and the data to new threats. And we'll consider how IBM has dramatically

© 2011 InformationWeek, Reproduction Prohibited

revamped DB2 security, including recent advances in DB2 security across the company's z/OS and iSeries as well as Linux/Unix/Windows (LUX).

The Evolution of DB2 Security

Exposure to Threats

Today's largest enterprises still rely on one of the industry's oldest and most established databases to store their most sensitive and business-critical data. DB2 has traditionally been at the heart of the data center, literally and figuratively. DB2 on z/OS and iSeries were the very definition of a "moat"-based security model, with a single application interface and local administration. The database served a limited number of applications, all confined to the corporate data center. A firewall separated the company from the rest of the world, and the internal network topology further cordoned off DB2 from general WAN connections. The database was simply more difficult to get to, and in most cases was not accessible from Internet-facing applications.

But adoption of DB2 on iSeries in virtual server environments, including "Blue Cloud" deployments of DB2 databases on Amazon's EC2 platform, the z/VM hypervisor and WebSphere Web App Server on z/OS, has changed the DB2 security model. The moat is gone and along with it the perimeter security concept. Ten years ago, most people thought mainframes and the iSeries were dead, but they continue to thrive in virtual cloud environments—with increased exposure to attacks.

From General to Targeted Attacks

DB2, especially on the mainframe and iSeries, has been overlooked by many authors of malware and remote exploit code. And that's not a joke about nobody writing exploit code in Cobol. The platform in general just has not been targeted to the extent that Microsoft products have been.

The ubiquity of Windows, and the ease with which SQL Server and Windows platforms were compromised, provided a greenfield of victims for malware targeting Microsoft products. A single virus or worm infects millions of databases. In contrast, because each of DB2's three platforms—z/OS, iSeries and LUW—behave slightly differently, the odds that a single exploit would work across all DB2 databases were diminished. Attackers want maximum effect for minimum work, and DB2 was simply more work with less likelihood of success.

© 2011 InformationWeek, Reproduction Prohibited

Now, however, targeted attacks against companies, individuals and foreign governments are common. Advanced persistent threat (APT) has entered the security professional's vocabulary. Opportunistic attacks written to compromise any vulnerable system have given way to focused attacks on specific targets. Consider for a moment that we have seen Stuxnet malware designed and written to attack both Windows and obscure SCADA systems used in nuclear facilities. DB2 is an attractive target, given its ubiquity in *Fortune* 2000 companies.

DB2 has had fewer recorded problems, especially critical issues as cataloged by the National Vulnerability Database, than other databases. Part of this is perception, as DB2 has suffered plenty of buffer overflow and access control weaknesses. But IBM has not been under the same degree of scrutiny as other database vendors, and has had the luxury of addressing code defects in house before they could be exposed publicly.

However, as the company adds features, integrates acquired technologies and makes new deployment options available, there is no reason to think DB2 security would remain immune to common attacks and public scrutiny.

Focus on the Insider

As a result of the lack of emphasis on Internet-based threats, the DBA, not an external attacker, historically has been considered the principle threat to DB2. It's a dirty little secret in the mainframe world that any skilled DBA could not only gain access to sensitive information, but could do so without being detected. Regulatory compliance and controls verification, not security, drove most DB2 security innovation. While most database vendors scrambled to provide vulnerability assessment and critical security patches to deter external attackers, DB2 customers focused on auditing for compliance and insider threats. In response, customers began requesting better logging services to detect administrative misuse and implementation of controls for compliance. Label security and the evolution of the security administrator (SECADM) accounts are two more examples of where IBM was focused.

When you take these factors into account, it's easy to see why IBM's vision of database security differed from that of the rest of the industry. IBM has been slow to build additional security measures into DB2, or create supporting security systems. Until recently, IBM has leveraged third-party products to close security gaps. But the reality is that DB2 faces the same security threats as every other database, and customer demand for safeguards is intensifying.

© 2011 InformationWeek, Reproduction Prohibited

Security Technologies

Native DB2 Tools

IBM began supplementing database security features in 2007 with a steady series of data and application security acquisitions, including Guardium, Netezza, Ounce Labs, Princeton Softech and Watchfire. With these and a few incremental product enhancements, IBM has closed all the major gaps in its security portfolio. Integrating these tools with Tivoli infrastructure management, security fits easily with workflow and compliance systems already in place.

Access controls and user authorization top the list as IBM's front-line defenses for data and database usage. The company also offers:

- Encryption. DB2 has offered column-level encryption for many years, and with Version 9 added table-level encryption of data as well. DB2 also provides some internal key management services, and encrypts different tables and data partitions under different keys.

- Labels. Label security provides fine-grained access control for column data. Rather than seeing all rows in a column, users are restricted to subsets according to their roles. Data can be classified and labeled according to type and sensitivity, and access assigned accordingly.

- Separation of admin roles. Introduction of the SECADM role allows for separation of duties between security tasks and day-to-day operations.

- Native audit. This capability and, to a lesser extent, event monitors allow for auditing of specific user actions and event types. The audit logs are used for change control verification and compliance reporting. Unfortunately, though, these tools impact database performance negatively—they were not designed to collect all events and queries, and are difficult to manage.

IBM has significantly augmented and improved upon these native capabilities; it has greatly enhanced database security, largely through its recent acquisitions. Ironic though it may be, the biggest advance in DB2 security ever is still largely unknown to DB2 customers. The acquisition of Guardium, with its suite of discovery, assessment, monitoring and auditing capabilities (more on that later), provides several critical security tools. What's more, it offers protection across z/OS, iSeries and LUX platforms. Let's look at how these acquisitions provide better security as DB2 has become increasingly exposed to attack.

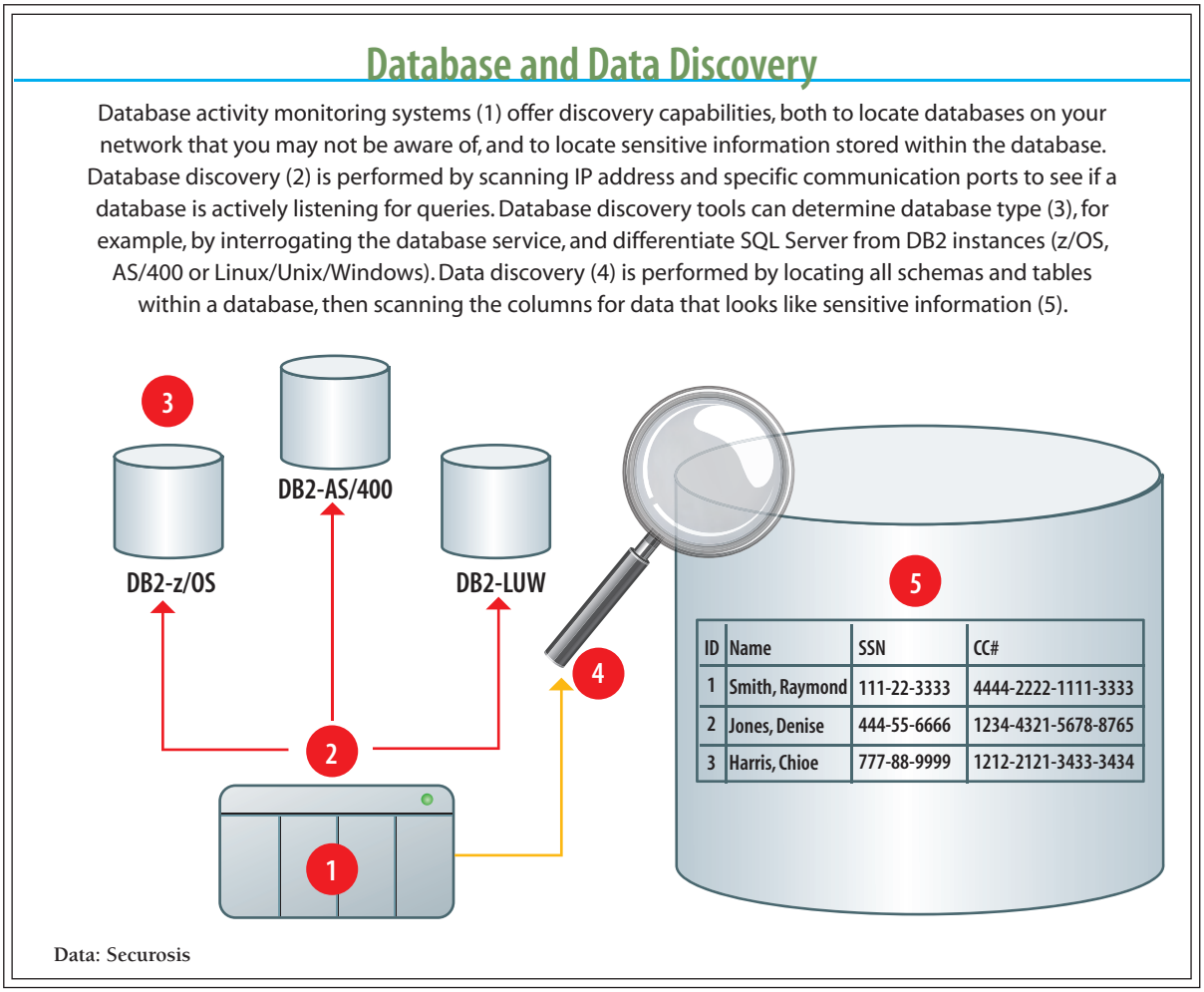
© 2011 InformationWeek, Reproduction Prohibited

Data and Database Discovery

While we equate database security with data security, the two are not the same. Knowing what data should be encrypted, what tables should be kept secret or even what transactions should be audited is predicated on knowing where sensitive information resides.

Database administrators who manage data warehouses or SAP installations can tell you it's next to impossible to be certain what information they hold and where, when it's spread across 40,000 tables in multiple databases. Production data is copied into replicated databases for failover protection, hot standby virtual instances and even test environments. When you con-

Figure 1



© 2011 InformationWeek, Reproduction Prohibited

sider the hundreds or thousands of databases in your IT environment, it's no wonder accurate discovery and identification is so challenging.

The first step for data protection and governance is to locate and identify sensitive information (see Figure 1, previous page). Customer information, employee information, medical information, financial information or any other data of value is likely subject to regulatory controls.

With Guardium, IBM offers database and data discovery tools for all versions of DB2 as well as other relational databases. Guardium's Classifier detects databases on a network, and can locate all database types within a supplied set of IP addresses and port numbers.

Classifier uses 'crawler' technology that finds all tables within the database and then optionally crawls the content within the tables. It returns the location and type of sensitive data it discovers, including database, schema and column information. It can classify data and build an inventory list of all sensitive data. And you can schedule it to run at off-peak times so it doesn't interfere with ongoing operations.

For each type of sensitive data it detects, Classifier can restrict access control to bring data security into compliance with standards. In addition to scanning content, Classifier also examines structural information—metadata, such as the name of the column or data type and size.

Once data has been discovered, Guardium makes policy enforcement a lot easier. Guardium's Classifier can alter data security settings as data is discovered through its discovery policy interface. Or, if your access controls dictate label security, the product can use scan results to create row, column or user security labels within DB2. Similarly, it can use scan results in conjunction with IBM's Optim Masking to specify transformation masks on personal information to obfuscate data as it is displayed, for users who don't need to see the actual data. (Data masking substitutes faux data to the user, or truncates it—showing, for example, only the last four digits of a credit card number.)

Monitoring and Blocking

Database activity monitoring (DAM) is unique in that it verifies database usage. Auditing shows us what happened; monitoring evaluates activity as it occurs, and can be set to react to events in near real time. It generally establishes a baseline of "normal" activity, monitors all attempts to

© 2011 InformationWeek, Reproduction Prohibited

access the database and issues alerts on and/or blocks suspicious activity, such as an unauthorized attempt to modify the database or access certain information (see Figure 2, below).

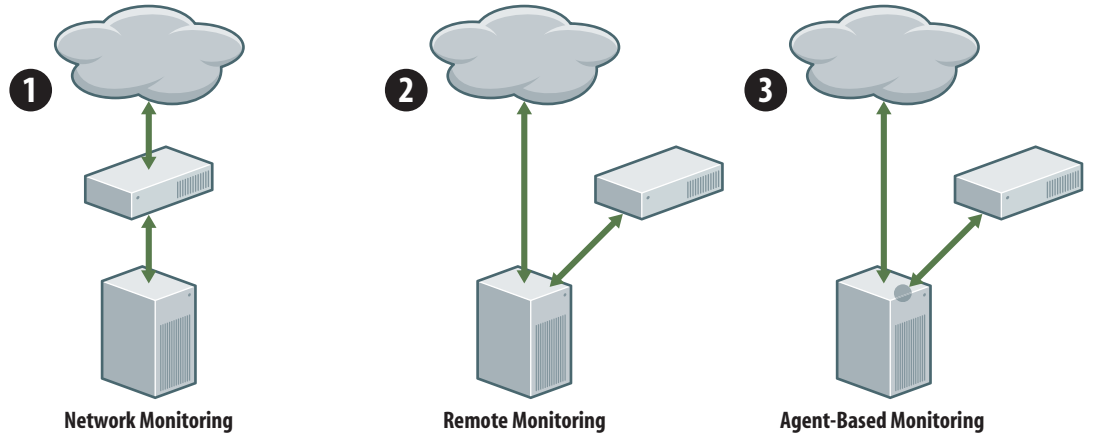
DAM is used to detect anomalous queries that indicate a database attack or other forms of misuse. It differs from native auditing in several important ways, as it:

- Detects access to data (i.e., Select statements), as well as alterations to data and structure
- Offers near real-time analytics and response
- Provides several forms of query and database usage analysis
- Can be deployed to block unwanted statements
- Requires fewer resources of the target database system than native auditing requires

Figure 2

How Database Monitoring Works: Basic Collection Techniques

Database activity monitoring leverages three methods to collect user activity: network monitoring, remote scanning of the audit trail and agent-based event collection. Network monitoring (1) is the easiest to use, has zero impact on the database, but does not capture all activity. Remote scans (2) collect all user and system activity without the aid of an agent, but require the use of native database auditing. Agent-based deployments (3) offer the broadest range of event-collection options, but must be installed and maintained on the database system. All three options are used today, often simultaneously, as each offers a unique advantage.



Data: *InformationWeek Analytics*

© 2011 InformationWeek, Reproduction Prohibited

Some features of DAM are similar to those of intrusion-detection and -prevention systems, but DAM offers database-specific security benefits. For instance, it:

- Works at the application layer, leveraging application context and transaction processing. This means DAM can detect logic flaws and enforce business process controls.

- Parses SQL statements in such a way as to detect unauthorized requests, SQL injection attacks and subversion of the application requests. Guardium deploys as a database firewall to block or perform connection resets to thwart anomalous queries.

- Creates baseline of user activity and will alert on legitimate sessions or actions that are out of the behavioral norm. Behavioral monitoring compares current user and group activity with known trends to detect insider misuse and hijacked accounts.

- Inspects query results and can detect misuse of privileges—for example, if a customer service representative attempts to view all customer records, or a hospital employee is looking at celebrity patient data.

- When deployed as an agent, sees all console and administrative activity. In this way, no database activity passes unnoticed, regardless of the protocol or service used to access the system.

Another advantage is DAM's ability to block statements—in near real time—that are deemed malicious. Blocking (see Figure 3, next page) is a desirable feature for many customers to address SQL injection attacks and to temporarily protect database features until patches can be installed. Blocking must be used cautiously, as false positives can have catastrophic effects on database operations: Applications fail, customers get angry and you're faced with a giant mess to clean up. But for some applications, especially those that hold credit card or other financial information, preventing data exposure is more critical than the occasional query failure.

Database Assessment

Most z/OS and iSeries administrators don't get excited by assessment tools. When you are responsible for only one or two database installations, it's just not that challenging to check for patches and configuration settings. But for DB2 admins on LUW platforms, with hundreds of databases to administer, periodic assessments are a huge amount of work. And let's face it, looking through user permissions settings is about as interesting as watching paint dry. The

© 2011 InformationWeek, Reproduction Prohibited

more tedious the task, the more likely you will overlook incorrect settings. Automated scans are faster, can be tuned to focus on a handful of important configuration items, and produce reports for security and audit staff without the need for administrative support.

Database assessment is about ensuring the basic preventative security measures are in place. Assessment tools verify the three most critical considerations for databases: testing configuration settings, verification that security patches are in place and auditing of user permissions.

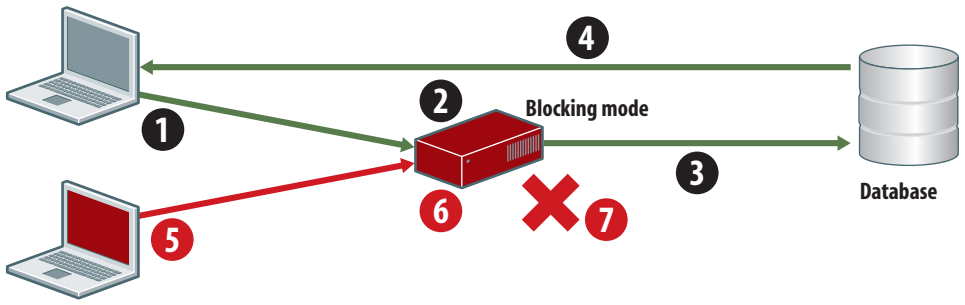
But generic operating system and network assessment tools only scratch the surface, collecting just what can be found in files or from the network port, neither of which is adequate for security and compliance testing. Database assessment brings both a depth and breadth of analysis to configuration and permissions testing not possible without access to and understanding of the database system tables.

For example, while you can externally determine the major revision of the DB2 instance without login credentials, you can't always determine which FixPak has been applied. Similarly, user permissions are defined within the database, and are available only through system queries.

Figure 3

Blocking Unauthorized Database Queries

Database activity monitoring (DAM) systems are deployed as an "out-of-band" witness of database transactions, or "in-line," acting as proxy for database queries. The out-of-band deployment is most commonly used for monitoring database queries only. In-line monitors, shown in this diagram, perform their analysis before a query reaches the database, offering protection from SQL injection and other types of database attacks. When a user makes an authorized query (1), the DAM device analyzes the request (2) and passes it on to the database (3), which returns the data to the user (4). If a user makes an unauthorized request (5), the DAM device analyzes (6) the query and blocks it (7) from reaching the database.



Data: *InformationWeek Analytics*

© 2011 InformationWeek, Reproduction Prohibited

Guardium provides database assessment for all three platforms and all supported versions of DB2. In terms of configuration and authorization assessment, it offers:

- **User permissions and roles.** A periodic review is necessary to verify users have only the permissions they need to perform their jobs, and that administrative privileges are locked down. But, as a practical matter, without automated filtering and reporting, a security review is impossible when you multiply hundreds of permissions by the thousands of users in your enterprise. Guardium examines authorization settings on a per-user/per-role basis to simplify reviews.

- **Database configuration.** Basic checks ensure the system and schemas are not available to the public, look for blank or default passwords and examine authentication settings. More advanced checks include network connection settings, JDBC configuration, audit buffer sizing, XML functions and other services that are common targets for attackers. The assessment policies list CERT and MITRE critical vulnerability advisories, as well as IBM best security practices.

Patch Management

Database vulnerabilities are common, and vendors issue patches frequently. Most zero-day attacks, such as SQL injection and buffer overflows, don't have specific workarounds, so you must patch quickly. For midsized and large enterprise IT organizations, just discovering which machines have been patched is difficult enough. Moreover, patches to the underlying operating system are integral to database security and must be maintained as well.

Its July 2010 BigFix acquisition provides IBM with a general patch management service across all the DB2 platforms. When the BigFix technology is used in conjunction with Guardium's assessment capability (see Figure 4, next page) to detect database patch revisions, both database and operating system patches can be managed from a single location.

BigFix does not provide database patch and configuration testing for DB2. But it does provide a management framework and a single pane of glass for monitoring and reporting on patching efforts for the database and the underlying operating system. Guardium's assessment results feed into patch management or other trouble-ticketing systems to initiate the work order, and BigFix manages the process and reporting.

© 2011 InformationWeek, Reproduction Prohibited

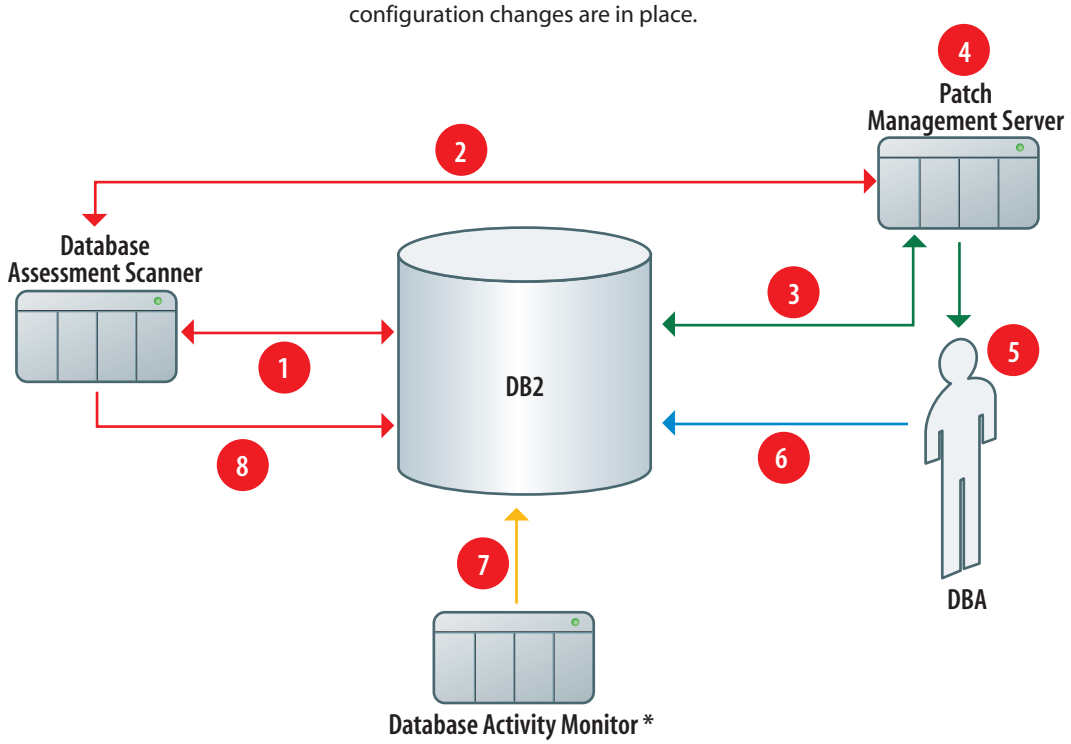
Auditing

DB2 provides auditing features native to the database. These features capture session-based information (e.g., Connect), user actions (e.g., Update), administrative actions (e.g., Grant) and metadata changes (e.g., Alter Table). But they don't capture all SQL statements, and they miss some administrative activity as well.

Figure 4

Database Assessment and Patch Management

Database assessment, monitoring and patch management tools commonly work in conjunction with each other. Database assessment scanners identify deficiencies in configuration and missing security patches (1). Missing patch information is passed (2) to a patch management server, which handles the workflow process for OS or database patch installation (3) and reports (4) when tasks are completed. Configuration issues are passed to the database administrator (5), who changes database settings to meet security requirements (6). The database activity monitoring tool (often the same appliance as the assessment tool) monitors (7) the administrative queries to ensure the changes were made by the correct administrator and performed according to specifications, and the database was restarted to make the changes effective. Subsequent database assessment scans (8) verify patches have been installed and configuration changes are in place.



Data: Securosis

* Often the same appliance as the assessment scanner

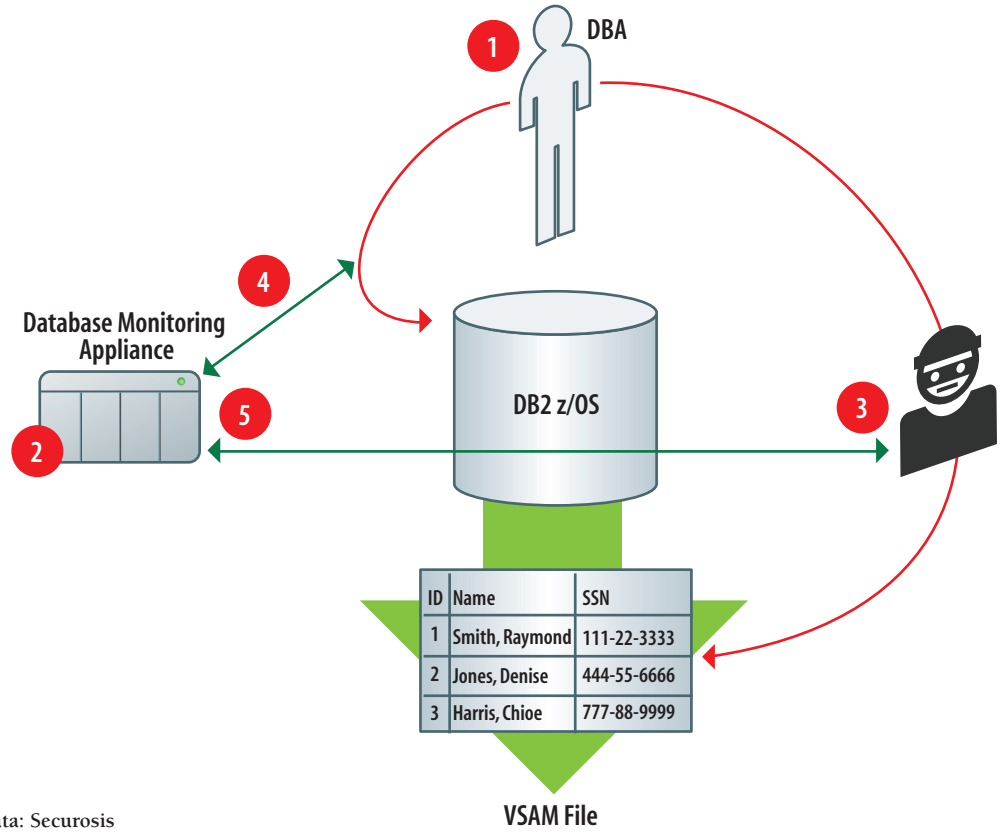
© 2011 InformationWeek, Reproduction Prohibited

Capturing all DBA events is essential to detecting insider misuse. Regulations such as PCI DSS and Sarbanes-Oxley require organizations to verify operational controls are in place and effective exactly for this reason. Also, not every DBA wants to use native audit or event monitors. Auditing slows performance and is difficult to set up. The audit trail is stored in the database, thus competing for disk and processor resources. For these reasons, audit is used selectively, or not at all.

Figure 5

How Database Auditing Counters the Insider Threat

Detecting misuse and verifying separation of duties are the two principle goals of database auditing. Audit trails, created by the native database features, don't capture all system events. And with platforms like DB2 on z/OS, administrators can bypass (1) the database engine and directly access VSAM storage files. Database activity monitoring tools (2) install an agent (3) on the operating system that captures direct file access—as well as database access (4)—and records these events (5) in a secure audit trail in a remote appliance or service.



Data: Securosis

© 2011 InformationWeek, Reproduction Prohibited

AME was designed by IBM to fix some of the shortcomings of conventional audit and event monitors, but it missed the mark in several respects. AME does not see direct file access for DB2 on z/OS, its trace-based event collection does not perform particularly well and it still stores data in the database.

Guardium provides auditing capabilities, and reduces setup and performance impact on target databases. Guardum's agent captures all data access, including file-based access on z/OS file, as it hooks into the operating system and intercepts file and database commands (see Figure 5, previous page). It can collect activity and create an audit trail, and provide built-in reports for specific compliance initiatives.

By collecting audit events independently of the DBA and storing a secure copy of audit data within the appliance, Guardium meets separation of duties requirements for regulatory compliance. It provides ad hoc reporting and analysis across all nodes, and can stream events to SIEM and log management systems.

© 2011 InformationWeek, Reproduction Prohibited

SECURITY dark READING
Protect The Business Enable Access

Want More Like This?

Making the right technology choices is a challenge for IT teams everywhere. Whether it's sorting through vendor claims, justifying new projects or implementing new systems, there's no substitute for experience. And that's what ***InformationWeek Analytics*** provides—analysis and advice from IT professionals. Our subscription-based site houses more than 900 reports and briefs, and more than 100 new reports are slated for release in 2011. ***InformationWeek Analytics*** members have access to:

Research: Why Security Technologies Are Failing Us: We're pouring billions of dollars into security products that just lead to increased complexity and exposure. In this report, we get to the root of the problem and provide concrete steps to take now.

Best Practices: The New Perimeter: It's time for a smarter, stronger, data-centric perimeter design that musters controls commensurate with your data's value. Follow our nine-step program to zero in on attackers' activities.

Strategy: Database Access Control: Some users have more privilege than they need for business purposes. Here, we examine management of user access to database functions.

Strategy: Responding to a Database Compromise: Criminals are after your corporate databases—and sometimes, despite your best efforts, they get what they're after. Find out how to determine what was breached and how to protect your assets going forward.

Strategy: Oracle Security: Oracle now offers an extensive range of optional security tools, including Transparent Database Encryption and Secemo firewall technology. Learn how to use them.

PLUS: Signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.

For more information on our subscription plans, please CLICK HERE

© 2011 InformationWeek, Reproduction Prohibited