Database Security & Auditing

Jeff Paddock
Manager, Enterprise Solutions

September 17, 2009
285 million records were compromised in 2008
Agenda

- The Threat Landscape
- Meeting Mandatory Compliance Requirements
  - Or Why Audit Databases?
- Database Security 101
- Auditing Databases
- Securing the Database
The Threat Landscape
Overview: Data Breaches

- Who is behind data breaches?
  - 74% external sources
  - 20% insiders
  - 32% business partners
  - 39% multiple parties

- What’s involved in a data breach?
  - 67% significant error
  - 64% hacking and intrusion
  - 38% incorporated malicious code
  - 22% abuse of privileges
  - 9% physical threats
  - 91% of records stolen linked to organized crime

Source: Verizon 2009 Data Breach Investigation Report

2008 Top Vulnerabilities Exploited:
- Unauthorized access via default accounts
- SQL injection
Publically Reported Data Breaches 2009 (Jan 1 – Apr 1)

Total Incidents: 131
Total Records Affected: 1,762,453

The following graphs show data loss incidents by data type and by business type over the period of this report.
Common Attack Vectors in 2008

Source: Verizon 2009 Data Breach Investigations Report
Costs to the Breached Organization

- $202 per record breached
- 2008 average total per-incident costs were $6.65 million
- More than 84% of cases involved organizations that had had more than one data breach in 2008
- 88% of all cases in this year’s study involved insider negligence

---

2009 Annual Cost of a Data Breach Study
(Ponemon Institute)
These Guys Want Your Data
Meeting Mandatory Compliance Requirements

OR

Why Audit Databases?
Compliance is More Critical than Ever!

A recent, independent survey that AppSec conducted found the following:

- Over 40% reported a failed security OR compliance audit in the past two to three years.

- One-third of enterprise respondents failed a security audit of some type (HIPAA, FISMA, SOX, etc.)

- Nearly 40% of respondents failed a HIPAA audit, the second-highest rate of failure for audits. Other common failures were internal audits, GLBA, PCI and FISMA.

Source: Application Security, Inc./Enterprise Strategy Group (Released 12/11/08)
## Regulatory Compliance Challenges

### SOX
- § 302-4: Quarterly Evaluation of Internal Controls over Financial Reporting (ICFR) mandates proper segregation of duties and restricted access controls

### PCI
- **Requirement 2**: Do not use vendor-supplied defaults for system passwords and other security parameters
- **Requirement 6**: Develop and maintain secure systems and applications
- **Requirement 7**: Restrict access to cardholder data by business need-to-know

### HIPAA
- 45 CFR § 164.308(a)(4), § 164.312(c)(1), § 164.308(a)(4), and 164.312(a)(1)
- Restrict authorized access to ePHI
- Instrument policy and procedures to restrict access to ePHI

### FISMA | NIST 800-53
- IA-1: Identification and Authentication Policy and Procedures
- IA-2: User Identification and Authentication
- IA-4: Identifier Management
- AC-1: Access Control Policy and Procedures
- AC-2 Account Management
- AC-3: Access Enforcement
- AC-5: Separation of Duties

### DIACAP | DISA STIG
- Access for Need-to-Know (ECAN)
- Least Privilege (ECLP)
  - Separation of Duties and Least Privilege
  - Privileged accounts are accessible only by privileged users
  - Use of privileged accounts is only for privileged functions
- Privileged Account Control (ECPA)
Compliance Demands on Database Security

Compliance Requirements
- Data lives in DB apps (90%+):
  - Privacy / confidentiality
  - Integrity
- Compliance must be:
  - Repeatable
  - Demonstrable
  - Automated

Increasingly Focused Attacks
- Directly on applications (75%+!)
- Including insiders (80+%!)
- Financially motivated

Demand for Pervasive Access
- By anyone
- To any application
- Increasingly direct
## Compliance and Database Security

<table>
<thead>
<tr>
<th>Audit Requirements</th>
<th>SOX</th>
<th>PCI</th>
<th>HIPAA</th>
<th>FISMA (NIST 800-53)</th>
<th>GLBA</th>
<th>BASEL II</th>
<th>DIACAP (DISA-STIG)</th>
<th>NERC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete Inventory of In-Scope Databases</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Vulnerability and Configuration Assessment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>User Entitlement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Threat Monitoring</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Privileged Activity Monitoring And Separation of Duties</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Database Security 101: Vulnerabilities & Countermeasures
Common Database Threats

Database Vulnerabilities:
- Default accounts and passwords
- Easily guessed passwords
- Missing Patches
- Misconfigurations
- Excessive Privileges

External Threats:
- Web application attacks (SQL-injection)
- Insider mistakes
- Weak or non-existent audit controls
- Social engineering
# Database Vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>Oracle</th>
<th>Microsoft SQL Server</th>
<th>Sybase</th>
<th>IBM DB2</th>
<th>MySQL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default &amp; Weak Passwords</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Patchable Vulnerabilities</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Misconfigurations &amp; Excessive Privileges</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Database Vulnerabilities: Weak Passwords

- Databases have their own user accounts and passwords

<table>
<thead>
<tr>
<th></th>
<th>Oracle</th>
<th>Microsoft SQL Server</th>
<th>Sybase</th>
<th>IBM DB2</th>
<th>MySQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default &amp; Weak Passwords</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Database Vulnerabilities: Weak Passwords

- Oracle Defaults (A Few Examples)
  - User Account: system / Password: manager
  - User Account: sys / Password: change_on_install
  - User Account: dbsnmp / Password: dbsnmp

- Microsoft SQL Server & Sybase Defaults
  - User Account: SA / Password: null

- Legacy Applications
  - Commonly use Weak Passwords

- User’s
  - Choose Favorite Things – Often not complex
Database Vulnerabilities: Passwords

- It is important that you have all of the proper safeguards against password crackers because:
  - Not all databases have Account Lockout
  - Database Login activity is seldom monitored
  - Scripts and Tools for exploiting weak passwords are widely available
Database Vulnerabilities: Missing Patches

- Databases have their own Privilege Escalation, DoS’s & Buffer Overflows

<table>
<thead>
<tr>
<th></th>
<th>Oracle</th>
<th>Microsoft SQL Server</th>
<th>Sybase</th>
<th>IBM DB2</th>
<th>MySQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patchable Vulnerabilities</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>
Database Vulnerabilities: Missing Patches

- Privilege Escalation
  - Become a DBA or equivalent privileged user
- Denial of Service Attacks
  - Result in the database crashing or failing to respond to connect requests or SQL Queries.
- SQL Injection & Buffer Overflow Attacks
  - Result in an unauthorized user causing the application to perform an action the application was not intended to perform.
  - Can allow arbitrary commands to be executed
    - No matter how strongly you’ve set passwords and other authentication features.
## Database Vulnerabilities: Misconfigurations

- Misconfigurations can make a database vulnerable

<table>
<thead>
<tr>
<th></th>
<th>Oracle</th>
<th>Microsoft SQL Server</th>
<th>Sybase</th>
<th>IBM DB2</th>
<th>MySQL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misconfigurations &amp; Excessive Privileges</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Database Vulnerabilities: Misconfigurations

Misconfigurations Can Make Databases Vulnerable

Oracle
- External Procedure Service
- Default HTTP Applications
- Privilege to Execute UTL_FILE

Microsoft SQL Server
- Standard SQL Server Authentication Allowed
- Permissions granted on xp_cmdshell

Sybase
- Permission granted on xp_cmdshell

IBM DB2
- CREATE_NOT_FENCED privilege granted (allows logins to create SPs)

MySQL
- Permissions on User Table (mysql.user)
Database Vulnerabilities: Misconfigurations (con’t)

- Excessive Privileges
  - Objects, Roles, Users
  - Inheritance

- Lack of Account Settings
  - Password Length, Expiration, Account Lockout, etc

- Access Controls
  - User Authentication
Auditing Databases
Auditing Databases – Where to Begin

- **Discovery**
  - Don’t rely on port mapping
  - Unknown Databases
  - Inventory Assets

- **Perform Baseline Assessment and Pen-Test**
  - Best Practices

- **Prioritize and Address Results**

- **Perform Regulatory or Security Assessment**
  - SOX, HIPAA, PCI-DSS, GLBA, FISMA, SAS 70
  - NIST 800-53, SANS, DISA-STIG
  - Include known Vulnerabilities
Auditing Databases – Next Steps

- **Separation of Duties**
  - Avoid using DBA
  - If not
    - Require Screen Shots or Physical Documentation
    - Witnesses
    - “Chain of Custody”

- **Change Management**
  - Total Population of Changes
  - Who did it, When, Using what?
Results

- **Output**
  - Detailed for Technical staff
  - Executive Summary
  - Typically difficult to Interpret without DB knowledge

- **Prioritize**
  - Severity
  - Policy requirements

- **Verify Remediation**
Securing the Database
Developing a Risk Framework

Assess Security Posture
- Assess database security risks
- Determine impact
- Establish and prioritize work

Measure Impact
- Document risks and controls
- Align business and IT goals
- Develop business case

Deal with Impact
- Direct costs
- Indirect Costs
- Cross-departmental buy-in

Establish Controls
- Facilitate accountability
- Establish reporting framework
- Implement access controls
- Integrate policies and procedures

What’s likely to happen
- Opportunity level
- Expertise required – business
- Expertise required - technical
How Do You Secure Databases?

- Start with a Secure Configuration
  - Make this part of your SDLC
  - Use Industry Accepted frameworks
    - NIST 800-53, SANS, CIS

- Stay Patched
  - *Stay on top of all the security alerts and bulletins*

- Implement the Principle of Least Privilege
  - *Review User Rights to ensure all access is appropriate*
How Do You Secure Databases?

Defense in Depth / Multiple Levels of Security

- Regularly scan your databases for vulnerabilities
  - Fix the problems reported!

- Implement database activity monitoring…
- ...and database intrusion detection
  - Especially if you can’t stay patched!

- Encryption of data-in-motion / data-at-rest
Automating Database Security, Risk & Compliance

- Manually assessing database security, risk & compliance is a time-consuming and costly process…even for SMEs!
  - Identify Vulnerabilities: 8 hours per database
  - Locate Misconfigurations: 20 hours per database
  - Examine Access Controls and User Entitlement: 40 hours per database
  - Research and Implement Remediation: 60 hours per database
  - Make the process repeatable and consistent across the enterprise: Impossible

- Automated solutions provide significant benefits:
  - Labor and cost savings: 120+ hours reduced to minutes per database
  - Consistent, repeatable results across heterogeneous environments
  - Easy to use systems, don’t require deep database expertise to operate
  - Professional analytics and reporting: visualize results to gain real insight
  - Strong security controls: Authentication, Role based access control, segregation of duties
Automation: Do More, Understand More

- Analytics and new information views enhance audit capacity and ability to see strategic risk and enhancements within the database.

- Look for in-depth reports and easy-to-use dashboards to deliver comprehensive database security information.

- Deliver executive level information to maintain project support and justify budget.

- Custom reports help organizations understand the risk and compliance profile of each database.
 Importance of Automation

- **Save time and money** – reduce man hours from 120+ hours per database down to 10-20 minutes per database
- **Get immediate value** – Scan an entire environment in the time it takes to manually assess a single DB
- **Demonstrate continuous improvement** – Consistent process and quick results facilitate easy progress reporting
- **Reduce scope** - Automation can reduce complex tasks such as user auditing by telling you what you need to monitor, where need compensating controls
Example: Reviewing User Rights Manually

**BASELINE**
- Define Business Functions and Roles
- Map to data access based on need to know
- Identify which employees fall into each function/role

**REVIEW AND APPROVE**
- Review and approve the baseline outlined by Security Ops.

**REMEDiate**
- Take identified violations from the Audit and run through remediation process on excessive permissions granted to users, roles, or groups.

**VERIFY**
- Repeat audit process to analyze entitlements after remediation
- Compare with previous audit results to demonstrate progress

**AUDIT**
- Engage DBA’s to provide entitlement data
- Analyze entitlements and engage with all parties when needed to determine if access permissions are within policy

**1 - Document users, roles, groups and permissions (Business)**

**2 - Review and approve documented permissions (Security)**

**3 - Continuously audit users access to critical data (Audit)**

**4 - Conduct proper remediation if excessive permissions are identified (DBA & Operations)**

**5 - Ensure permissions remain accurate and within documented policy (Audit)**

**30-60 Hours / DB**

**40-80 Hours / DB**

**APPLICATION SECURITY, INC.**
Example: Reviewing User Rights with Automation

1. Document users, roles, groups, and permissions (Business)
2. Review and approve documented permissions (Security)
3. Continuously audit users access to critical data (Audit)
4. Conduct proper remediation if excessive permissions are identified (DBA & Operations)
5. Ensure permissions remain accurate and within documented policy (Audit)

REPEATABLE PROCESS
• Delta Reports against previous scans

5-10 Minutes / DB

PROVIDE EFFECTIVE PRIVILEGES AND OBJECT ACCESS REPORTS
• Role Inheritance
• Multiple Grant Paths to Privileges
• Excessive Privileges

EXPORT DATA TO BASELINE DOCUMENTATION FOR REVIEW AND APPROVAL

RUN VA AUDIT AND URR
• Vulnerability Details
• All Users in the Database
• All Roles in the Database
• All Effective Privileges for a Role

RUN USER RIGHTS REVIEW
• All Roles for a User
• All Effective Privileges for a User
• Object Access

EXPORT DATA TO BASELINE

Save 70+ hours per database in each audit

5-10 Minutes / DB
Database Activity Monitoring: Features and Benefits

- Separation of controls
  - Dedicated storage for audit records
  - Administration is centralized

- Minimal performance impact

- Easy to setup and configure auditing

- Cross-platform capable
  - Audit Oracle, MS SQL, Sybase, and DB2 identically

- Professional reporting
  - Aggregate data from many database sources

- Some add Intrusion Detection capabilities
  - Detect attacks and fire alerts to security systems
Database Activity Monitoring: Architecture Options

- **Network-based monitoring**
  - **In-line:** All network traffic passes through
    - Facilitates blocking and dropping of queries
    - Some overhead and risk of failure causing DoS
  - **Out-of-band:** Sniffs a mirror of the network traffic
    - Zero overhead and zero risk
    - No blocking, but can react to threats
  - Both methods only see what crosses the network

- **Host (agent)-based monitoring**
  - Many techniques for data collection
    - Memory sniffing, log scraping, native auditing
  - Sees all queries, regardless of source
    - Some performance overhead
## Database Activity Monitoring: Summary Reporting

### Threats by Severity

- **Low**: 18 occurrences (25.93%)
- **Medium**: 12 occurrences (25.93%)
- **High**: 16 occurrences (44.44%)

### Risk Levels
- **High**
- **Medium**
- **Low**
- **Informational**

### Summary Table

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk</th>
<th>Occurrences</th>
<th>Database Type</th>
<th>Host</th>
<th>Port</th>
<th>Instance</th>
<th>Database</th>
<th>Title</th>
<th>Last Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing OS Resources</td>
<td>High</td>
<td>6</td>
<td>Microsoft SQL Server 2005</td>
<td>127.0.0.1</td>
<td>0</td>
<td>JSHAUL0</td>
<td>master</td>
<td>Read sensitive OS files</td>
<td>Sep 29, 2008 1:03:48 PM EDT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>127.0.0.1</td>
<td>0</td>
<td>JSHAUL0</td>
<td>master</td>
<td>SAM database in registry accessed</td>
<td>Sep 29, 2008 1:03:48 PM EDT</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>6</td>
<td>Microsoft SQL Server 2005</td>
<td>127.0.0.1</td>
<td>0</td>
<td>JSHAUL0</td>
<td>master</td>
<td>Generic use of xp_cmdshell</td>
<td>Sep 29, 2008 1:03:48 PM EDT</td>
</tr>
<tr>
<td>Audit Events</td>
<td>Low</td>
<td>1</td>
<td>Microsoft SQL Server 2005</td>
<td>127.0.0.1</td>
<td>0</td>
<td>JSHAUL0</td>
<td>master</td>
<td>Accessing list of logins</td>
<td>Aug 27, 2008 1:18:03 PM EDT</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Medium</td>
<td>2</td>
<td>Microsoft SQL Server 2005</td>
<td>127.0.0.1</td>
<td>0</td>
<td>JSHAUL0</td>
<td>master</td>
<td>Log erasing using sp_cycle_errorlog</td>
<td>Aug 27, 2008 1:29:19 PM EDT</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>Medium</td>
<td>6</td>
<td>Microsoft SQL Server 2005</td>
<td>127.0.0.1</td>
<td>0</td>
<td>JSHAUL0</td>
<td>master</td>
<td>SQL injection in sp_MSdroproetry</td>
<td>Sep 29, 2008 1:03:48 PM EDT</td>
</tr>
</tbody>
</table>
Best Practices for Database Activity Monitoring

1. Log database login attempts, both successful and failed
2. Log changes to database schema (DDL commands)
3. Log database privilege / permission / authorization changes
4. Log database configuration changes
   • Authentication modes, password controls, remote access, auditing
5. Log password changes
6. Log changes to production data made by ad-hoc query tools (DML commands)
7. Log direct changes to System Catalog data
8. Log attempts to issue a known attack against the database
   • Buffer overflow, DoS, Privilege Escalation, SQL Injection, Password Attacks, Etc…
9. Log failed object accesses
10. Log database backup and restore operations
About Application Security, Inc.
Application Security, Inc. - Company Overview

- The Database Security, Risk, & Compliance (SRC) Leader
- Headquartered in NYC, USA
  - Representation worldwide
- Industry-leading solutions
  - Most awarded database security solution on the market
  - Solution of choice for auditors and security consultants
  - Industry’s largest database vulnerability knowledgebase
- Industry-leading customer base
  - 2,000+ customers, 250,000+ databases
- Strategic Relationships
  - DBMS vendors, integration partners, technology influencers
AppSec’s Team SHATTER

- Industry’s largest independent database security research team
- Responsible disclosure policy
  - Continual interaction with vendors to identify and mitigate vulnerabilities
- Industry’s most extensive database threat knowledgebase
  - 2000+ vulnerabilities, 1400+ checks, 1000+ rules
- Monthly ASAP Knowledgebase Updates
  - Mapped to various Commercial and Federal compliance regulations: DISA-STIG, NIST 800-53, SCAP (CVE, CCE, CPE), Common Criteria
- Frequently published database security experts
Additional Resources

Database Security Controls – a joint study by Application Security, Inc & Enterprise Strategy Group

McAfee Virtual Criminology Report 2008
www.mcafee.com

McAfee Unsecured Economies Report 2008
www.mcafee.com

2009 US Cost of a Data Breach Study
www.encryptionreports.com

http://securityblog.verizonbusiness.com

2008 KPMG Data Loss Barometer Report
http://www.kpmg.com
Additional Resources

Zero Day Threat, Acohido, Byron and Jon Swartz (USA Today security reporters)
http://zerodaythreat.com

Market Share: Database Management Systems Worldwide, 2007 (Gartner)
www.gartner.com

Privacy Rights Clearinghouse
www.privacyrights.org

Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy
Thank you!

Application Security, Inc.
1-866-9APPSEC (1-866-927-7732)
Sales@appsecinc.com

Please join us for an upcoming webinar!