Database Auditing: Best Practices

Rob Barnes, CISA
Director of Security, Risk and Compliance Operations
rbarnes@appsecinc.com
Verizon 2009 Data Breach Investigations Report:

285 million records were compromised in 2008
This Session’s Agenda

• **Introduction**
  – Database Vulnerabilities are the New Front-Lines
  – Factors that Drive Requirements for Database Auditing

• **Attacking Where the Data Resides**
  – Planning an Attack
  – Attacking Database Vulnerabilities

• **Database Auditing**
  – Securing Your Databases
  – Database Auditing and Forensics
  – Best Practices
## Recent Breaches

<table>
<thead>
<tr>
<th>Company/Organization</th>
<th># of Affected Customers</th>
<th>Date of Initial Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartland Payment Systems</td>
<td>100,000,000</td>
<td>20-Jan-09</td>
</tr>
<tr>
<td>Monster.com</td>
<td>Unknown</td>
<td>23-Jan-09</td>
</tr>
<tr>
<td>phpBB.com</td>
<td>400,000</td>
<td>5-Feb-09</td>
</tr>
<tr>
<td>University of Alabama</td>
<td>37,000</td>
<td>13-Feb-09</td>
</tr>
<tr>
<td>CVS Pharmacies</td>
<td>Unknown</td>
<td>18-Feb-09</td>
</tr>
<tr>
<td>Arkansas Department of Information Systems</td>
<td>807,000</td>
<td>20-Feb-09</td>
</tr>
<tr>
<td>Idaho National Laboratory</td>
<td>59,000</td>
<td>7-Mar-09</td>
</tr>
<tr>
<td>US Army</td>
<td>1,600</td>
<td>12-Mar-09</td>
</tr>
<tr>
<td>Symantec</td>
<td>200</td>
<td>31-Mar-09</td>
</tr>
<tr>
<td>Metro Nashville School/Public Consulting Group</td>
<td>18,000</td>
<td>8-Apr-09</td>
</tr>
<tr>
<td>Peninsula Orthopedic Associates</td>
<td>100,000</td>
<td>11-Apr-09</td>
</tr>
</tbody>
</table>

Etc, etc, etc.

Source: Privacy Rights Clearinghouse: [http://www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)
Databases Are Under Attack

- **February 2005 to March 2009**
- **Total Affected Customers:** 355,547,925+
  - Literally hundreds of incidents
  - Victims include financial institutions, government agencies, retailers, healthcare providers, universities, manufacturing, consulting and audit firms ….
- **Incidents reported almost every day**
  - Already over 100,000,000 records stolen in 2009!

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm
The Threats to Enterprise Data Continue to Rise

- The database security landscape has changed:
- Attacks are targeting the database where records can be harvested in bulk on a global scale
- Perimeter security measures are necessary but not sufficient
What Do The Numbers Tell Us?

- **84%** Percent of companies that feel database security is adequate
- **56%** Percent of the same companies that experienced a breach in the last 12 months
- **73%** Percent of companies that predict database attacks will increase

Enterprises are Plagued by a False Sense of Security

Don’t wonder if your data is protected, *Know* it’s protected
To Make Matters Worse - Threats Are Very Real

Database Security: Recent Findings

- Only 1 out of 4 databases are locked down against attacks.

Source: 2008 IOUG Data Security Report, Joe McKendrick, Research Analyst
Data Breach Costs Are Rising

253 million records breached
X 202 per record
------------------------------------------
Equals
------------------------------------------
$51.1 billion
breach related costs

Cost Per Exposed Record

<table>
<thead>
<tr>
<th>Year</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>$138</td>
<td>$181</td>
<td>$197</td>
<td>$202</td>
</tr>
</tbody>
</table>

Ponemon Research
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 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)
To Make Matters Worse - Threats Are Very Real

Database Security: Recent Findings

• One out of five respondents expects a data breach or incident over the coming year.
• “...few have addressed the key vulnerabilities stemming from exposure of data to internal sources.”
• “...only a minority has addressed security to monitor "super users"—such as administrators with heightened access privileges—either onsite or offsite.”

Source: 2008 IOUG Data Security Report, Joe McKendrick, Research Analyst
Database Vulnerabilities
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>Denial of Services &amp; Buffer Overflows</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Misconfigurations &amp; Privilege Management Issues</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Database Vulnerabilities: Default & 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: Default & Weak Passwords

• Oracle Defaults (hundreds of them)
  - 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

• 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 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>Default &amp; Weak Passwords</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Missing Patches</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.

- 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.
## 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>Default &amp; Weak</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Passwords</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of Services</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>&amp; Buffer Overflows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misconfigurations</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 Auditing & Forensics
Database Protection Planning: Auditing and Monitoring

1. **Access & Authentication Auditing**
   Who accessed which systems, when, and how

2. **User & Administrator Auditing**
   What activities were performed in the database by both users and administrators

3. **Security Activity Monitoring**
   Identify and flag any suspicious, unusual or abnormal access to sensitive data or critical systems

4. **Vulnerability & Threat Auditing**
   Detect vulnerabilities in the database, then monitor for users attempting to exploit them

5. **Change Auditing**
   Establish a baseline policy for database; configuration, schema, users, privileges and structure, then track deviations from that baseline
Auditing: Vulnerability Assessment & Activity Monitoring

- "Outside in" and "Inside out" scan of all database applications to assess:
  - Security strength
  - Database vulnerabilities
  - Application discovery and inventory
- Fix security holes and misconfigurations
- Develop policies based on results from scan to identify:
  - Database vulnerability
  - Roles and responsibilities functionality to segregate users
  - Compliance risk factors
- Auditing
  - Comprehensive reporting
- Real-Time Monitoring
  - Defend against misuse, fraud, and abuse from internal and external users
  - Monitor all user activity and system changes (DDL, DML, DCL)
  - Tune detection parameters to capture events while bypassing false positives
Database Security
Best Practices
### Data Security Risk and Compliance Life Cycle

<table>
<thead>
<tr>
<th>Lifecycle Component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover</td>
<td>Produce a database or asset inventory</td>
</tr>
<tr>
<td>Classify</td>
<td>Finds sensitive data to determine business value of systems and associated regulatory requirements</td>
</tr>
<tr>
<td>Assess</td>
<td>Scan databases for vulnerabilities, misconfigurations / configuration changes, and user entitlements</td>
</tr>
<tr>
<td>Prioritize</td>
<td>Combine info from classify and assess phases to determine what to fix, what to mitigate through compensating controls (monitoring), and in what order to do the work</td>
</tr>
<tr>
<td>Fix</td>
<td>Create and run fix scripts, apply patches, create monitoring policies to implement compensating controls</td>
</tr>
<tr>
<td>Monitor</td>
<td>Audit privileged access and access to sensitive data. Monitor for exploits and suspicious or unusual behavior</td>
</tr>
</tbody>
</table>
Best Practices Methodology
Database Security Best Practices

Assess Security Posture
- Assess database security risks
- Determine processes, applications and systems affected
- Prioritize risk and establish work plan

Address Risk
- Document risks and controls
- Align business and IT goals
- Develop business case for investment in security

Establish Controls
- Set responsibilities and accountability
- Establish mechanisms for reporting and assessment
- Apply the principle of least privilege and role based access controls
- Implement policies and procedures to minimize exposure

Implement Monitoring
- Implement the program
- Monitor risks and controls
- Distribute reports to provide perspective to executive teams
- Test and remediate
- Audit and attest
- Measure and monitor readiness
How Do You Secure Databases?

• Start with a Secure Configuration
• Stay Patched
  – Stay on top of all the security alerts and bulletins
• Implement the Principal of Least Privilege
  – Review User Rights to ensure all access is appropriate
• 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
Audit Your Database Environment TODAY!

**Check for object and system permissions:**
- Check views, stored procedures, tables, etc. permissions.

**Look for new database installations:**
- Specifically third party database installations.

**Search for users with DBA privileges:**
- This helps to detect intrusions, elevation of privileges, etc.

**Audit database configuration and settings:**
- If security configurations or settings are changed for instance by a system upgrade, patch, etc.

**Check database system objects against changes:**
- Detecting system changes you haven't applied could mean that a rootkit is present.
HOW TO: Protect Against Attacks

Set a good password policy:
• Use strong passwords or passphrases.

Keep up to date with security patches:
• Try to install patches as fast as you can. Database vulnerabilities are serious and sometimes a database server can be easily compromised with just a simple query.
• Always test patches for some time on non-production databases.

Protect access to the database server:
• Allow connections only from trusted hosts and block non used ports and outbound connections. Establish exceptions for special instances like replication, linked databases, etc.

Disable all non used functionality:
• Excess functionality can lead to vulnerabilities

Use selective encryption:
• At network level: use SSL, database proprietary protocols.
• At file level for backups, laptops, etc.
HOW TO: Protect Against Attacks

Set a good password policy:
• Use strong passwords or passphrases.

Keep up to date with security patches:
• Try to install patches as fast as you can. Database vulnerabilities are serious and sometimes a database server can be easily compromised with just a simple query.
• Always test patches for some time on non-production databases
HOW TO: Protect Against Attacks

*Protect access to the database server:*
- Allow connections only from trusted hosts and block non used ports and outbound connections. Establish exceptions for special instances like replication, linked databases, etc.

*Disable all non used functionality:*
- Excess functionality can lead to vulnerabilities

*Use selective encryption:*
- At network level: use SSL, database proprietary protocols.
- At file level for backups, laptops, etc.
HOW TO: Periodically Audit Database Systems

Check for object and system permissions:
- Check views, stored procedures, tables, etc. permissions. Check file, folder, registry, etc. permissions. Changes on permissions could mean a compromise or mis-configuration.

Look for new database installations:
- Third party products can install database servers and new installed servers could be installed with blank or weak passwords, un-patched, mis-configured, etc. Detect new database installations and secure or remove them.

Search for users with DBA privileges:
- This helps to detect intrusions, elevation of privileges, etc.
HOW TO: Periodically Audit Database Systems

Audit database configuration and settings:
• If security configurations or settings are changed for instance by a system upgrade, patch, etc. your databases could be open to attack. If they change and there wasn't a system upgrade then it could mean a compromise.

Check database system objects against changes:
• If you detect a change in a system object and you haven't applied a fix or upgrade to your database server it could mean that a rootkit is present.
Advantages of Off-database Auditing

- **Native database auditing has its disadvantages**
  - Must be enabled and configured on each system individually
  - Separation of controls/ Segregation of Duties?
    - Can be solved with audit management tools (aka Audit Vault)

- **Native auditing**
  - Can be disabled or deleted by attacker in the database
  - Most databases have NO auditing configured
Advantages of Off-database Auditing

• *3rd-party security tools provide improved auditing*
  • Most importantly, they protect and store the audit trail

• *Focus attention on critical issues*
  • Highlights potentially suspicious activity
  • Differs from volumes of audit logs
  • Operationally efficient
  • Indicates possible need for action
  • Helps eliminate false-positive responses
  • Preserves resources, staff, time and money
Audit & Threat Management Recommendations

- Perform Database Auditing and Intrusion Detection
  - Implement real-time monitoring
- Integrate with native database audit by scanning logs
- Integrate with audit management tools
- Implement real-time alerting (SIEM integration)
- Keep a library of best-practice implementation information
Database Security Info from AppSecInc

• White Papers
    • SQL Server Forensics
    • Database Activity Monitoring
    • Search Engines Used to Attack Databases
    • Introduction to Database and Application Worms
    • Hunting Flaws in Microsoft SQL Server

• Presentations
    • Protecting Databases
    • Hack-Proofing MySQL, IBM DB2, Oracle9iAS
    • Writing Secure Code in Oracle
    • Addressing the Insider Threat to Database Security

• Security alerts
  – www.appsecinc.com/resources/mailinglist.html
Additional Resources

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

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

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

http://securityblog.verizonbusiness.com

Security alerts:
www.appsecinc.com/resources/mailinglist.html
Questions?
– Vulnerabilities?
– Locking down the database?
Email our security experts at:
asktheexpert@appsecinc.com

blog.appsecinc.com
Database Security Best Practices with DbProtect