

Database Security Tips for 2012

2011 has been a banner year for data breaches. The spate of activity by hacktivist groups and nation-state attacks, as well as the overall number of records compromised has set a new high-water mark. Chances are you have heard about these high profile breaches in the media, perhaps within your own organization, or at home around the dinner table. What you may not be hearing about are details of how they happened, and more importantly, how they may impact you in 2012.

The escalating threat is being felt throughout every organization. Whether driven by external threats, insider threats, or auditor findings, the challenges of database security, risk and compliance have changed the key roles and responsibilities in many organizations.

As databases contain our most valuable economic, personal, and government information, it is critical to protect sensitive information in order to safeguard businesses, individuals, political systems, and human rights worldwide.

The following list highlights top security tips that IT professionals should include in their database defense strategy for 2012:

1. **Devise a Database Security Plan**
2. **Fix Default, Blank, and Weak Passwords**
3. **Regularly Patch Databases**
4. **Minimize Attack Surface**
5. **Review User Privileges**
6. **Locate Sensitive Information**
7. **Encrypt Sensitive Data at Rest and In Motion**
8. **Train and Enforce Corporate Best Practices**

1. **Devise a Database Security Plan**

When developing a database security plan, start with an established database checklist and customize it to the organization's needs. Don't try to build a program from scratch as it is too much effort and there are great free

resources out there that can be leveraged. Depending on the industry, there might be regulations to follow like PCI-DSS, SOX or HIPAA. DISA STIG is an excellent starting point. DISA (the Defense Information Systems Agency) publishes detailed guidance on how to secure and properly configure MS SQL Server, and Oracle, as well as generic guidance that can be applied to any database platform in use. (Download the database STIGs from DISA's website at: <http://iase.disa.mil/stigs/checklist/index.html>.)

Once a security and configuration policy is established, build a plan to roll it out. Pick one or two of the highest risk issues (such as default passwords and/or missing patches) and attack those first. As progress is achieved, layer on additional checks and tests. This approach will have a dramatic impact on security in the shortest possible timeframe. This process ensures the most critical issues are being resolved – instead of low-risk fixes that may seal a crack in the wall while leaving the front door wide open.

2. **Fix Default, Blank, and Weak Passwords**

Ensure that all databases have complex passwords and that default, blank, and weak passwords are eliminated. Make sure to use separate passwords for each instance and enforce and extend the same password policy that your organization is currently using to all network logins. If the database supports it, consider using network authentication, such as Active Directory, instead of username/password authentication.

3. **Regularly Patch Databases**

Typically, when a bug or vulnerability is discovered in an application, vendors will fix the bug and provide patches that are critical in the prevention of certain attack vectors perpetrated by hackers. While each vendor is on a different cycle, from a couple times a year, to a few times a month, these critical patches ensure that

vulnerabilities are addressed and remediated on a regular basis. Discovering and patching these vulnerabilities in conjunction with auditing and monitoring known unpatched vulnerabilities protects the database from threats.

These patches are well tested by vendors. The risk of getting hacked is higher than the risk of the patch breaking your application and staying on top of patches will strengthen the databases' security posture.

4. Minimize Attack Surface

Many database management system (DBMS) features provide database application developers with additional power. However, many of these features are optional and are not required by applications accessing a database. The DBMS ships with many features, packages, and modules that enable the easy development of powerful applications, but often those features remain unused. The more features a software package has installed or enabled, the more likely it is that some of these features will have flaws or allow for unexpected functionality.

5. Review User Privileges

Insiders pose a significant threat to sensitive enterprise information. This data ranges from proprietary research information, corporate best practices, Social Security and credit card numbers, as well as and other confidential personally identifiable information. Ensure that employees ONLY have access to the sensitive information they need to do their jobs, and nothing more. Conducting regular user entitlement reviews provides auditors, IT advisors, and consultants with a detailed view of an organization's data ownership, access controls, and rights to sensitive information. This process allows organizations to establish and document compliance with the segregation of duties controls required by industry and government regulations. These controls manage conflicts of interest and ensure employees do not have toxic privilege combinations that can lead to theft or other business disruptions.

- *Map Job Functions to Privileges on IT Assets* – Determine and document the access to IT resources required for each job function across the organization in a Least Privilege Policy. Build a process to ensure all employees are assigned the

documented privileges required to complete their daily job activities and nothing more.

- *Never Assign Privileges Directly to Guest Accounts or Public* – Restrict privileges to the specific roles and accounts that need them. Granting privileges to guest accounts or anonymous groups such as public (everyone) almost always leads to violations of the Principal of Least Privilege.
- *Untangle The Web of User Entitlements* – Whether it's done manually by hand, or automatically using software, organizations should continuously assess user entitlements to understand exactly what privileges are assigned to each employee. Having a detailed, accurate inventory of privileges allows organizations to weed out toxic combinations of privileges that may have been inherited over time.
- *Implement Compensating Controls for what cannot be fixed* - Monitor user privileges that cannot be modified or restricted to ensure data access isn't being abused or misused. Put the most scrutiny on the most highly privileged users and make adjustments to the Least Privilege Policy as required. Monitor users who are abusing access privileges,

5 Key Steps to Ensuring Database Security

In order to effectively secure their databases, organizations must address five critical requirements:

1. **Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.
2. **Eliminate Vulnerabilities:** Continually assess, identify and remediate vulnerabilities that expose the database.
3. **Enforce Least Privileges:** Identify user entitlements and enforce user access controls and privileges to limit access to only the minimum data required for employees to do their jobs.
4. **Monitor for Deviations:** Implement appropriate policies and monitor any vulnerabilities that cannot be remediated for any and all activity that deviates from authorized activity.
5. **Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.

such as stealing data, manipulating information, or even inadvertently mishandling information and create incident response triggers.

Establishing strong policy-based access and activity monitoring on critical systems forestalls an insider attack. Activity monitoring and auditing provides alerts on suspect activity allowing action to be taken in a timely manner. Database security solutions geared for the enterprise allow IT and security personnel to set different alert levels based on activity type. These alerts can be intelligently filtered and disseminated in a variety of formats and to defined groups or individuals based on pre-established policies

6. Locate Sensitive Information

It is imperative to know where all sensitive information resides on the network, and to secure the information in those databases first. Commonly, most organizations are unaware of all the data contained in databases, where all of their sensitive data resides in those databases, or are completely unaware of rogue databases on the network. This scenario can quickly lead to a data breach. To know where the most sensitive data resides, first conduct a comprehensive analysis of which users have access to each system, which data and functionality they can access, and verify that the level of access that has been granted is appropriate based on the user's business function. Forward-thinking organizations must proactively implement user entitlement best practices that ensure appropriate access and ownership rights are assigned to critical data. Failure to conduct a full user rights review increases an organization's risk of data access abuse and increases the risk of failing mandated compliance audits.

7. Encrypt Sensitive Data at Rest and In Motion

Never store sensitive data in clear text in a table in the database where any member of a DBA/IT team can access that sensitive data. Ensure that the information is encrypted and not allowed to travel on the network. By locking down database vulnerabilities and closely monitoring access to critical data stores, database professionals can discover attacks in time to stop them. Defense against a SQL injection attack requires a multi-layered approach, and protective measures should be architected with an end-to-end view, meaning that both the web application and the database infrastructure are scoped into the solution.

8. Train and Enforce Corporate Security Best Practices

Ensure that employees are aware of the organization's security best practices. Having an established training program and a consistently reinforced policy deters users from compromising sensitive information through human error. In addition, organizations can mitigate the effect of successful phishing attacks by detecting the suspicious activity in a timely manner. Database activity monitoring and auditing minimize the impact of such an attack.

To ensure that these unintentional violations do not occur, organizations should extend the critical protections in place at the network and web application layer to the database. Regular database security assessments including audit and pen tests, and misconfiguration checks should be performed to minimize these risks. In addition, activity monitoring can be implemented to guarantee that sensitive data is not unwittingly downloaded or transferred.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: www.appsecinc.com | www.teamshatter.com

For a free database vulnerability assessment visit: www.appsecinc.com/downloads/appdetectivepro

Follow us on Twitter: www.twitter.com/appsecinc | www.twitter.com/teamshatter

**APPLICATION
SECURITY, INC.**[®]
www.appsecinc.com