



Control Essentials

Database Security



Databases hold your most sensitive data and are one of the primary systems assessed by auditors to achieve compliance with key regulations such as SOX, PCI-DSS, GLBA and others addressing data privacy and security. This article describes an approach database administrators may use to achieve compliance and minimize the risk of data compromise.

Typical issues with databases

The following is a short list of common issues affecting databases we typically identify during vulnerability assessments and audits engagements:

- Improper authentication implementation
- Excessive user access privileges
- Database design/implementation vulnerabilities
- SQL injections
- Lack of audit trails
- Protocol vulnerabilities

Achieving Security and Compliance

The approach proposed achieves database security and regulatory compliance by implementing a methodical framework and minimizing the risk of security breaches:

Database Enumeration and Discovery

The first step is to ensure you have a complete inventory of all databases containing sensitive data. There are many automated tools including freeware software that performs database discovery. Once all the databases have been identified, you will need to decide whether a database should be added to the inventory. In order to do so, you will have to refer to your data classification policy. If the database contains non-public information as defined by your data classification policy, then it should be added to the inventory. This step should be performed on a regular basis due to constant changes made to systems and network.

Vulnerability Assessment

A vulnerability assessment is required to identify the security issues affecting your databases. This includes the assessment of the following:



- Overall operating system security
- Database installation configuration on the operating system:
 - File privileges for database configuration files and executables
 - Services provided by the database engine
 - Users used by the engine to run
- Internal database configuration including:
 - Database version
 - Database objects (tables, store procedures, trigger, queries) access control configuration
 - Groups and users defined and related access permissions
 - Audit trails configuration
 - Password policies configuration
- Encryption: Unless PCI is the driving force for your organization's security, you do not have to encrypt your databases. However, data encryption is an additional security layer that hackers would have to bypass after they broke into the database. Encryption can be also applied to database connections in order to protect data confidentiality while in transit.

Configuration Standards and Database Hardening

The results of the vulnerability assessment are the foundations of the remediation plan and database hardening. Upon discovery of the vulnerabilities affecting the databases, an action plan should be created to not only remediate but also prevent and promptly detect security problems:

1. Ensure that all the verified vulnerabilities are corrected.
2. Harden the database by applying security best practices, including: apply patches, assign to users only minimum permissions required, turn off unused services, and change the default configuration to more secure settings
3. Document all the exceptions such as customizations or deviations from the best practices that are required by the business to function
4. Test the changes to prevent business disruption
5. Develop configuration standards that outline the database security configuration including the deviations identified. This document will be your security baseline.

Database Monitoring

Once the database has been locked down, it should be ensured that audit trails are generated and maintained for any database activities that may impact the integrity and/or confidentiality of sensitive data. At least the following events should be audited:

- Failed logon attempts
- Successful logon attempts
- Configuration change
- User management activities
- If possible, activity information at the query level would provide a lot of useful data

In addition to being a key compliance requirement, the presence of audit trails is also important for forensic investigations. As a rule of thumb, the last three months of logging information should be easily accessible and information older than three months can be backed up with the rest of the data and retrieved only if necessary.



Ongoing Reassessment

On an annual basis, the database configuration should be compared against the baseline and any exceptions identified should be documented and reported. Exceptions should be classified as incidents (unauthorized change) or as an authorized change and supported by evidence. The configuration standards should be updated accordingly to the changes made as they become part of the baseline.

Ultimately, it would be a good practice to perform a semiannual or annual entitlements review of databases users.

Conclusions

Maintaining regulatory and security best practices is not an easy task, but with a proper plan and processes that include hardening and change control management, your organization can secure sensitive data and keep it safe from malicious hackers.

ERM wants to hear from YOU....

With this edition of our newsletter, we're rolling out a new format and new features. Tell us what you think!

What features or topics would you like to see covered in future issues? Who else should receive this newsletter?

Your feedback is welcome and encouraged. Please send your comments to editor@emrisk.com.

Enterprise Risk Management: *At a Glance*

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions.

Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

Services

- IT Security
- Regulatory Compliance
- IT Audit
- Computer Forensics
- Risk Management
- Attestation

Certifications

- Certified Public Accountant (CPA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Certified Information Technology Professional (CITP)
- GIAC Security Essentials Certification
- GIAC Systems and Network Auditor
- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)

Some of our Clients

- ABN-AMRO Private Banking
- Bacardi-Martini, Inc.
- Bancafe International
- Banco Industrial de Venezuela
- Banco ITAU
- Bank United
- Caja Madrid Bank
- Carnival Cruise Lines, LLC
- CitiBank
- Coconut Grove Bank
- Commerce Bank
- E-data Financial
- Florida International University
- Florida Power & Light Company
- Heico Aerospace
- Helm Bank
- Knight Ridder
- Nova Southeastern University
- Rinker Materials
- Rudy, Exelrod & Zieff, LLP
- Seabourn Cruise Line
- TecniCard, Inc.
- The International Bank of Miami
- TransAtlantic Bank
- U.S. Century Bank

For more information, visit www.emrisk.com

E-mail: info@emrisk.com

Phone: 305-447-6750

800 Douglas Road

North Tower, Suite 835

Coral Gables, FL 33134

enterprise risk management

The Control Professionals