

Research Note

Date: January 29, 2008
Title: Security Criteria For Selecting A Database
Written by David Mortman

Summary

Opinions and vendor hype about the inherent security of various database products abound. Understanding a vendor's overall approach to security assurance is critical for selecting database – and other – products that meet an organization's security standards. This research note outlines an approach that will help organizations evaluate objectively how security is integrated into commercial database solutions. It recommends seven key points to consider when making a critical database purchasing decision: vendor disclosure of his product's particular vulnerabilities and their severity; relevant security features; integrated product development security processes; ongoing vendor-provided software assurance; patch remediation logistics; independent product vulnerability assessment; and product administration usability.

The Issue

Over the last couple of years, security issues and data breaches have focused attention on how organizations protect their information. As a result, security practitioners, especially at large companies, are increasingly being asked for input into the product purchase lifecycle. Perhaps the most common question they are asked is: Which product is the most secure? This is hardly a new question and has been debated for years with strong camps arguing the relative merits of Microsoft Windows vs. UNIX, proprietary vs. open-source and Internet Explorer (IE) vs. Firefox (and before that IE vs. Netscape). Lately the debate has extended itself to databases with emotional arguments coming from all sides. The issue has become even more controversial with increasing customer concern about security and vendors posturing over whose software is more secure.

The reality is that there is no easy answer to this debate; each organization needs to evaluate its needs objectively, decide what risks are acceptable, and choose the appropriate software accordingly. A consistent, objective approach in evaluating database security can help organizations make an informed and thoughtful decision. There are seven key points to consider when making a critical database purchasing decision:

1. Product Security Features
 - a. What are the security features and are they relevant?
 - b. How flexible are the security features? Can they be fine-tuned to a level of granularity that satisfies current and prospective information security and availability needs?

- c. Is security turned on by default, that is, is the product locked down upon installation? If not, is it easy to lock the product down? Keep in mind that the existence of a feature is no indication of its usefulness
 - d. Are specifically desired features, such as encryption, designed and implemented well – and in accordance with published standards?
 - 2. Vendor Disclosure of Vulnerabilities
 - a. Is the vendor open to discussing the security issues customer is facing?
 - b. Does the vendor realistically and consistently rate the severity of their vulnerabilities (e.g., by using Common Vulnerability Scoring System (CVSS))?
 - 3. Secure Development Practices
 - a. Is security addressed at all levels of the development process? Poor security hygiene results when an organization incorporates security elements at the end of a development or deployment process. It is essential that security be integrated as part of the overall software development lifecycle.
 - b. How is security expertise seeded organizationally? Are developers familiar with secure programming fundamentals?
 - c. Does everyone who is part of development receive appropriate and timely training? Creating requirements that security be integrated into the lifecycle and that developers need to attend courses on secure application coding will reduce both security issues and long-term database maintenance costs.
 - d. Does the vendor use automated tools to detect vulnerabilities in code? Is a spectrum of tools employed in addition to human review?
 - e. Is there external validation of the security of the product through third party penetration testing, code reviews, or certification such as Common Criteria?
 - 4. Ongoing Software Assurance
 - a. Does the vendor have an effective process for keeping customers informed about vulnerability alerts?
 - b. Does the vendor have a long-term plan for supporting the product?
 - c. How comprehensive and thorough is software testing prior to product release?
 - 5. Vulnerability Remediation
 - a. What does the overall database patch management process look like? Since the SQL Slammer worm appeared on the computer systems of organizations back in 2003, applying the latest database security patches should have evolved from being a fire drill to being part of everyday business.
 - b. How often does the vendor provide patches and is it on a schedule that meshes with your business process?
 - c. Are patches for critical vulnerabilities provided in a timely fashion?
 - d. How often does the vendor re-issue patches?
 - e. Does the vendor have a clean, easy to understand process for acquiring, testing, and installing patches? Are patches tested adequately before their release? How are fixes validated?
 - f. Does the patch documentation clearly indicate which component is affected by the vulnerability being patched?
 - g. What is the vendor's vulnerability disclosure process?
 - 6. Independent Vulnerability Assessment

- a. Have you verified the effectiveness of the security features of the products you are considering? Have you reviewed third party and external certification documentation for security features that are relevant to your business environment?
 - b. Does the vendor offer tools to verify configurations and missing security patches? Third party tools can also be used to aid independent analysis of the product's reliability.
 - c. Has the vendor submitted its products for external security validations such as Common Criteria and FIPS? Have those validations been obtained on current releases? Has the vendor committed to obtaining those validations for future releases?
7. Product Administration Usability
- a. Are product guidelines, templates, case studies, or reference frameworks available that ease the task of securely configuring the product ?
 - b. Does product documentation include warnings about potential technical difficulties?
 - c. Does the vendor support user group discussions about changes in features and different use case scenarios?
 - d. Does the vendor charge customers for security patches, product documentation, and best practices guidelines?

Conclusion

The crown jewels of an organization are kept in databases. Selecting a secure and reliable database product is essential to reduce the risk of data compromise – and damage to the organization's reputation for trust and integrity. Measuring the quality of a piece of software by the metric of number of vulnerabilities alone is doing a disservice to customers. The number of patches is in itself a red herring. Understanding a vendor's overall approach to security assurance is critical for selecting secure software. The seven-point checklist of security criteria recommended here will help organizations make appropriate choices that lead to understanding a vendor's overall approach to security assurance.