



The new Sun Storage Systems.
Storage made simple, with high-performance ZFS.

GET IT NOW »

InformationWeek

BUSINESS INNOVATION POWERED BY TECHNOLOGY

Database Servers: Candy For Hackers

Sensitive information and poor security administration make tempting targets.

By Ericka Chickowski, [InformationWeek](#)

June 20, 2009

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=218100141>

Good hackers today are businesspeople, assessing each target for the simplest and most profitable attack scenarios. These days, there are probably no plumper targets than enterprise databases.



Databases house companies' easiest-to-sell confidential data: customer lists, payroll records, and many other structured inventories of sensitive information. Database administrators tend not to be steeped in security practices, and the databases themselves are frequently tied to Web applications that have turned out to be easy to hack.

In its annual breach study, Verizon Business' computer forensics team reported that databases made up 30% of data compromises in 2008. Worse, database breaches accounted for 75% of all records reported breached. Because sensitive information is often found in a single database, a single breach can lead to major damage.

"When you get down to it, a large percentage of the security threats potentially go after the database," says Rich Mogull, analyst and founder of Securosis, an enterprise security consulting firm. Most [information security](#) practitioners grow up on the networking side of IT and know little about database technology, adds Mogull. And a recent Forrester Research study found that database administrators spend less than 5% of their time on database security.

"I'd say that of the calls I take on this subject, at least two-thirds of the time, the database folks aren't involved," says Jeffrey Wheatman, Gartner's research director of information security and privacy. "I think that's a problem, because when you're monitoring or securing something you don't really understand, you need to bring in a subject-matter expert to help you."

Many database security vulnerabilities are caused by simple lapses in security. In a 2008 poll, the Independent Oracle Users Group found that 26% of organizations take more than six months to install security patches on [Oracle](#) databases; 11% have never patched them. "Production databases don't get patched nearly often enough, because they're busy database servers and people will say, 'If it isn't broken, don't fix it,'" says Adam Muntner, a partner at QuietMove, a vulnerability assessment firm.

Companies often make mistakes that leave databases vulnerable, such as

Get the full-length
Analytics
Report:

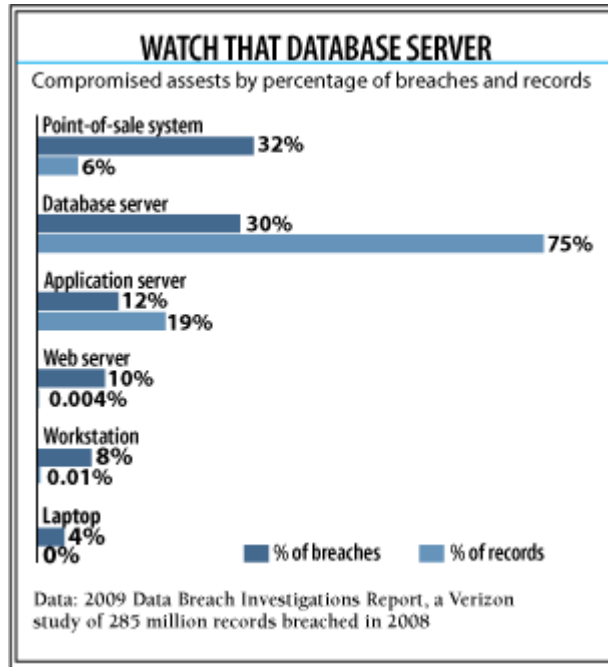
[Why Your
Databases Are
Vulnerable To](#)

<http://www.TakeABackup.com>

leaving test databases on production servers or linking sensitive data to easily hacked Web-facing applications. "I think that the biggest threat to databases is Web applications and the business logic vulnerabilities within them," Muntner says.

[Attack -- And What You Can Do About It](#)

Close ties with Web applications can make databases vulnerable to SQL injection attacks, whereby attackers input strings of SQL code into weak Web applications fields. They can then [raid](#) the database linked to a specific Web application, and also use the link between the Web application and the database to launch more expansive attacks on entire database servers. According to IBM's ISS X-Force security research unit, [SQL](#) injection flaws last year were the Internet's most commonly exploited Web application vulnerability, growing by 134% over 2007.



ALL ABOARD! The OMS Regional Whistle Stop Tour! The premier online marketing educational event 11 cities across the U.S. May 5 - July 2

Click to get a 20% discount

[LEARN MORE](#)

OnlineMarketing.com
Hosted by

Copyright © 2009 [United Business Media LLC](#). All rights reserved.

<http://www.TakeABackup.com>