FEDTECH
Solutions Report

5 Next-Level Data Consolidation Tips

Follow these five data management tips for a successful consolidation project.

Threat Prevention»

Feds Focus on Web App Security

Security-conscious federal agencies look to lock down the growing number of mobile web apps.

Karen D. Schwartz

posted June 19, 2012 | Appears in the Spotlight on Client Computing Strategies issue of the *FedTech Magazine* e-newsletter.

Related Articles
Serving Up Anytime, Anywhere Apps Over a Private Cloud
Review: Symantec Endpoint Protection.cloud
Policies, Not Tools, Drive Cloud Security
FedBytes: Is Communication the Best Defense Against Cyberthreats?
How to Build a Security Dashboard
Editors Picks

How Adopting Shared Services Boosts Efficiency
Software for Monitoring and Management
Next-Generation Tech Gets Agencies Ready for Enterprise

The Census Bureau has moved many of its applications to the web. And like most agencies, Census experiences the growing pains and security concerns that go along with that evolution.

“With web-based apps, we have become more concerned about how we are coding the applications, because that seems to be a target for attackers,” says Timothy Ruland, the agency’s chief information security officer. “We’re also concerned about mobile devices accessing the web-based applications.”

The National Nuclear Security Administration (NNSA), with its focus on research, development and security, also builds and hosts many web-based applications. In fact, Travis Howerton, the agency’s chief technology officer, was first hired at the agency in 2002 as a web application developer, making NNSA one of the most aggressive in adopting the web application model.

Howerton, along with Anil Karmel, NNSA’s management and operations chief technology officer, are understandably concerned about web application security.

“Being that we are primarily research-based, we tend to take a cutting-edge approach to security in our enterprise, given the mission of our agency. It is imperative that we employ the correct tools and approaches to ensure that our apps are secure,” Karmel says.

Top Priority

86%
The percentage of web applications that are vulnerable to an injection attack, where internal databases are accessed through a website

SOURCE: 2011 Top Cyber Security Risks Report (HP)

Jeff Wilson, principal analyst with Infonetics Research, says there are many reasons why agencies should make securing web applications a top priority. Mobile versions of web apps are yet another stream of code that must be maintained, managed and checked for vulnerabilities.

"Custom code, or simply poor coding that leaves vulnerabilities in the code during development, can cause real security problems," Wilson says.

"If you have the right tools and can get at the code to fix the problems, you'll be in pretty good shape. But if you don't have access to the code because the application was outsourced or built on a platform where you are at the mercy of the platform developer, it's more difficult to find and fix vulnerabilities," he adds.

At Census, web application security is multifaceted. The first step includes educating programmers about potential threats and ways to review code. One tool the programmers use to help with that task is *HP's WebInspect,* a web application security assessment program.

As CISO, Ruland has also led the development of security configuration baselines at Census for mobile devices that can be used for agency business. To help control those devices, Census has implemented a mobile device management system from *Sybase Afaria*.

But some of the most important strategies don't involve technology at all.

"The most important things are education and collaboration," says Stephen Moore, chief of the Application Services Division at Census. "In the past year, my staff and Tim's staff have begun to collaborate and communicate more, and we're getting the other areas involved as well."

NNSA's Howerton agrees that web application security processes are every bit as important as the technology.

"We make sure that all development uses managed frameworks, separates duties in the code base, separates the presentation tier from the data tier, and uses parameter-based queries to prevent SQL injection–type attacks on the front end," he explains.

NNSA also employs the latest web application security technology. In addition to using load balancers for packet inspection, NNSA uses a combination of penetration testing tools to both internally and externally validate the applications for production. The agency also employs web application firewalls, products that Howerton says are getting smarter all the time.

"We're starting to see tools that will go through your source code or your compiled executable code and figure out how to exploit it dynamically, and then create automatic application firewall rules that then feed their product to protect your specific application from the specific vulnerabilities they face," he says.

Tools of the App Security Trade

There are several possible tools that agencies can use to ensure the security of their web apps, including penetration testing and web application firewalls.

Penetration testing tools, such as *IBM Rational AppScan* and Tenable Network Security's *Nessus ProfessionalFeed*, actively try to find vulnerabilities in web apps caused by problems such as cross-site scripting and SQL injection. They work by simulating the methods real attackers might use, but without actually damaging the web application. Typical features of these tools include both static and dynamic testing, content audits (for example, for adult content and personally identifiable information), and the ability to pinpoint specific lines of code causing problems. They are also used for compliance auditing.

Web application firewalls are just that: firewalls that protect web applications. Marketed by providers such as *Fortinet*, *Barracuda Networks*, *F5 Networks*, *WatchGuard Technologies* and *Imperva,* these products block threats such as cross-site scripting, SQL injection, buffer overflows and denial of service cookie poisoning. They can also help organizations comply with the Payment Card Industry Data Security Standard. Other features include load balancing and Secure Sockets Layer offloading and acceleration.

Although these tools are invaluable, there is also great value in old-fashioned ingenuity, says Jeff Wilson, principal analyst at Infonetics.

“Whatever investment you make in web application security, there will still be bugs you miss,” he says. “Consider trying the crowdsourcing approach, like Google does. They pay a bounty to anyone who finds bugs in their code.”

Storage

Which Disaster Recovery Site Strategy Is Right for You?

Be sure to factor in the agency's objectives and continuity needs before making an...

NAS Creates Lots of Storage in a Small Space

Network-attached storage devices can fulfill the needs of both large and small...

more »

Networking

New 802.11ac Wireless Standard Promises Gigabit Speeds

With more traffic going wireless, agencies can look to the next Wi-Fi standard for...

How to Make a Smooth Switch to IPv6

Determine agency needs and existing environments before jumping into the new...

more »

Mobile & Wireless

New 802.11ac Wireless Standard Promises Gigabit Speeds

With more traffic going wireless, agencies can look to the next Wi-Fi standard for...

3 Ways the Military Is Using Mobile Applications

How technology is powering the Army, Air Force and Veterans Affairs.

more »

Hardware & Software

Maximizing Windows 8 Security Features

Three core enhancements can improve security.

Review: Symantec Endpoint Encryption Device Control, Full Disk Edition and Removable Storage Edition 8.2.2

Get control of your organization’s data security policies.

more »

Infrastructure Optimization

Security

Storage

Networking

Mobile & Wireless

Hardware & Software

Management