COMPUTERWORLD
The voice of the ICT community

SITEMAP | SUBSCRIBE | NEWSLETTERS | CONTACTS

SEARCH

HOME | NEWS ▾ | TECHNOLOGY | SECURITY | **DEVELOPMENT** | NETWORK & TELCO | SPECIAL | MANAGEMENT | CAREERS ▾ | NEW MEDIA | FRYUP | EVENTS ▾

FRIDAY, 20 AUGUST 2010

FOLLOW US ON TWITTER | | BECOME A FAN ON FACEBOOK | | RSS

CodeScan targets US with security audit apps
PHP tester added to ASP product

BY ULRIKA HEDQUIST | AUCKLAND | FRIDAY, 12 SEPTEMBER, 2008

EMAIL   PRINT

Auckland-based CodeScan Labs has released a tool for testing source code for security vulnerabilities. In addition to CodeScan for ASP, released in 2005, the company recently released a version for the PHP scripting language.

Peter Benson, the CEO of the company, founded security consultancy Security-Assessment.com, which was acquired by Asia Pacific services firm Datacraft for NZ$5 million in January this year. Benson has since left Security-Assessment.com and is now working full-time on CodeScan.

The company employs six staff, but expects to double that number within a year, says Benson. Industry veteran Chip Dawson has also come on board as sales director.

The CodeScan tool enables companies to audit web applications for security weaknesses by testing the source code, says Benson. The advantages over traditional, manual penetration or web application testing, which tends to be a tedious process, are huge, he says.

Web applications, in particular, are in the risk zone because they are "handcrafted" and often make use of many different languages and components, such as plug-ins, he says.

According to Benson, 80% of websites go live without being tested for vulnerabilities. He thinks the reason for this is that the majority of developers are not trained to test code from a security point of view — nor are they required to. Development is usually focused on usability and functionality — that is what the clients ask for, he says.

If security is part of the system development lifecycle, this could significantly reduce cost as well as exposure, he says.

The tool will find, for example, SQL injections; cross-site scripting; badly written code and insecure use of code, says Benson.

There is still a lot of "band-aid work" going on, such as relying on firewalls and penetration detection tools, says Benson. But if a company's website is not secure, and it is attacked, all the company will know is who attacked the site and how often the site is attacked.

"But why not build a secure website in the first place?" he says.

Many companies seem to be hoping for a "silver bullet". "But there is no silver bullet," he says.

Accountability for data breaches has got to come into the picture, according to Benson.

If a website is hacked, who is responsible — the third party developer or the company that commissioned the site? If you are hiring third party developers to build your site, at least scan their code, he says. IT security is just another business risk that needs to be managed, he says.

The increasing pressure of security compliance on large enterprises as well as small companies, and the Payment Card Industry (PCI) data security requirements, create demand for tools such as CodeScan, says Benson.

"The opportunities for this market are unlimited," he says.

The company is primarily targeting the heavily regulated US and European markets. New Zealand is still lagging behind when it comes to regulatory compliance, he says. Benson expects to see both large enterprises and development companies adopt the technology.

CodeScan is doing ongoing research and updates the system regularly, so that customers can re-scan their code on a regular basis.

The company won a grant from FRST (Foundation for Research, Science and Technology) which allowed it to get R&D started, says Benson.

CodeScan is currently working on a .Net version, which will be released in the end of October.

PHP support for Oracle, SQL Server, and DB2 will be released later this month, he says.

EMAIL
PRINT
SHARE THIS STORY WITH: