City of Brisbane
Agenda Report

TO: Honorable Mayor and City Council

FROM: Caroline Cheng via Clay Holstine, City Manager

DATE: Meeting of February 17, 2009

SUBJECT: Updating the City's Web Site

CITY COUNCIL GOALS:

To provide for effective and efficient delivery of City services. (1)
To encourage community involvement and participation. (15)

PURPOSE:

To inform the City Council of the current security issues having to do with the City's Web site and the police grant which the City recently received from the State.

RECOMMENDATION:

For Council to hear the report and provide guidance on how to proceed.

BACKGROUND:

In April of 2008, the City's Web experienced the first of many hacking attacks, resulting in information missing on some webpages, to other pages appearing to be blank. After consulting with a Web security expert, it was discovered that the City's database server had thousands of areas in the current code that allowed for malicious code to be injected by hackers. The frequency of these SQL injection attacks became rampant in the summertime. (SQL stands for Structured Query Language, and is itself a programming language for querying and modifying data and managing databases).

The City is currently utilizing the web development services of e21, an integrated marketing agency firm based in Fremont, CA. e21 provides all the back-end programming, which authorized City staff is able to update using e21's e-Volve Content Management (CM) software. The contract between the City and e21 dates back to April 4, 2003, in which the City paid e21 $19,500 for the design and implementation of the City's first Web site.

DISCUSSION:

For several months, staff has implemented a defensive strategy that involves locking down the Web site so that it is in a read-only state. Authorized Web site Administrators "unlock" the site when changes need to be made, and once those are completed, the site is locked back up to prevent any malicious code from coming through. However, there is no guarantee against malicious code penetrating the database during this window of time. Requests for the Web site to be unlocked and updated occur nearly on a daily basis.

The way in which the code is currently written allows hackers many opportunities to gain control of the City's database, rendering it inoperable. These gaps can be closed if more secure code can replace that which is currently in place. Due to the high cost that would be needed for programmers to re-write the flawed segments of code, this may be an opportunity for the City to have a new Web site built from scratch.

The City recently received a federal grant, where $50,000 was designated for the purpose of improving communications between the Police Dept. and the citizens. This grant money can be applied towards an improved City Web site, which is hoped to increase the level civic engagement between the community and the City of Brisbane.

FISCAL IMPACT/FINANCING ISSUES:

None at this time. Should the Council decide to pursue the building of a new City Web site, ideas for layout, appearance, and total budget may progress via a Council Subcommittee.

MEASURE OF SUCCESS:

Heightened security for the City's Web site, and that it will be the community's go-to spot for the latest information from the City.

Management Analyst

City Manager

ATTACHMENTS:

A – Redmondmag.com Article "SQL Injection Attacks on the Rise"

ATTACHMENT A

Redmondmag.com

News

SQL Injection Attacks on the Rise

by Stephen Swoyer

August 13, 2008

According to security researcher MessageLabs, the number of SQL injection attacks spiked sharply last month, helping account for a near doubling of the number of malicious Web sites it identified and blocked each day. This amounts to a record-high threat level, the security researcher said.

Why SQL injection attacks and why now?

"An emerging theme for threats [in July] seems to be new variations on old attack methods," said Mark Sunner, chief security analyst for MessageLabs, in a statement. "Following on from June, Web-based malware continues to be a treacherous threat and organizations would be smart to build their Web security defenses in preparation for what could be on the horizon."

If July was any indication, more SQL injection, cross-site scripting and other familiar attacks could be on the horizon.

SQL injection vulnerabilities are the very stuff of low-hanging fruit. They're almost certainly widespread, stemming as they do from design trade-offs, development deadlines, functional requirements, a lack of imagination or developer indifference.

They're also easy to test for, security experts said, in part because of a bevy of free, publicly available testing tools, including a plug-in for the popular Firefox Web browser. Consequently, researchers said, the onus is on development teams to proactively identify and patch SQL injection flaws before attackers -- using, in some cases, the same tools -- beat them to it.

"The root cause is unvalidated input, which can lead to SQL injection, among other things, including cross-site scripting, passive manipulation, and other things," said a CISSP with a prominent consulting and services firm who asked to remain anonymous. "The point is that there are tools out there [such that] if you point them to a Web site, they will try [injecting SQL into] every Web site they can find. There's even a Firefox extension."

That's part of the rub, according to this CISSP. "This is just one of several tools designed for site designers to scan their own Web sites. But that's part of the problem: It's freely available and anyone can use it -- the bad guys can use it just as easily as the developers themselves."

How does a SQL injection vulnerability become a reality? This CISSP -- who, in a former career, logged almost a decade as a software engineer -- said it's a question of dueling pressures. "Developers are under pressure to release software that fulfills functional requirements. Security requirements are generally not part of functional requirements. The No. 1 rule is to release the software that does its job by this date. If you can't do anything else, do that," he said. "The way we'd like to see development going is you'd like to have a security guy involved from the beginning. You'd like to have developers knowing or caring enough, or having time [enough], to test these things themselves."

Not that attackers are foregoing innovation altogether, of course. According to

MessageLabs, spammers are ceaselessly innovative. They'd previously exploited Google's hosted applications (i.e., Google Docs, Google Pages and Google Calendar) to disseminate spam, for example. Last month, spammers were targeting Google's "Sites" feature, which lets them build URLs (derived from Web pages consisting of random letters and numbers) that are more difficult to block using conventional anti-spam tools.

"Google Sites is yet another way that spammers have programmatically defeated CAPTCHA [Completely Automated Public Turing Test to Tell Computers and Humans Apart] mechanisms, a validation technique that is designed to defend against automated sign-up tools frequently used by spammers by requiring the user to enter a string of letters," Sunner said. "While Google Sites spam accounts for only 1 percent of all spam currently, we anticipate that this technique's popularity will rival that of its predecessors, Google Docs, Calendar and Pages spam. If this is the case, then we may see spam levels increase in the months ahead."

Stephen Swoyer is a contributing editor for several 1105 Media sites. He's based in Athens, Georgia. You can contact Stephen about SQL Injection Attacks on the Rise at swoyerse@yahoo.com.

PRINT THIS PAGE NOW

BACK TO PREVIOUS PAGE

TOP