



Subject: What Holes are in Your Applications?

August 31, 2006

Dear Real Estate Executive,

As a rule, hackers look for the easiest way to penetrate a network. Quite often, that entry point is through an application that has security vulnerabilities. Mitigating application security issues requires a holistic process that addresses education, process and quality assurance.

You should consider some basic application development fundamentals before hiring a vendor or developing an application yourself. First, a typical application developer does not have significant knowledge of networking or security. Therefore, training and educating developers on how to avoid coding vulnerabilities into applications can more adequately address the root source of application security issues. One important point of interest is that to develop more secure code, there is generally no additional overhead in skill, time or lines of code. Once trained and educated, developers embrace this knowledge and tend to incorporate these practices into everything they code.

Second, policies, procedures and guidelines need to be developed that specifically outline the expectations of custom coding. These administrative items unify the development platform, define expectations of coders and give the organization established "teeth" to fall back on when suspect code is discovered or expectations are not met by the developers.

Finally, the developed code needs to be subjected to a quality control and assurance process in an effort to minimize security vulnerabilities. Quality control and assurance should minimally be applied to all applications that interact with the public and all critical custom applications that are internal to the organization.

So what questions do you need to ask your vendors about application development?

1. Have your programmers been trained in secure programming techniques?

2. Did the training cover vulnerabilities specific to my environment, type of application and development process?
3. Is encryption and decryption carefully implemented? Is all sensitive information stored in an encrypted form?
4. Do you have source control and bug tracking systems? These are indicators that security problems can be tracked to their root causes.
5. Does every design decision include a security analysis?
6. Do you find security vulnerabilities before they become problems or only after? Are all audit reports documented and tracked to completion?

If the answers to these questions are positive, then you can significantly affect the overall posture of applications, which essentially follow the same guidelines traditionally used to address network security. Once these holistic processes are integrated and operational, the general risks associated with custom coded applications can be more effectively managed.

Application vendors for our industry need to continue to embrace high standards for information security in their development efforts. They also need to continue to develop applications with more security features and functions that will allow you to manage security more effectively within our businesses. Locally, if you introduce home-grown applications to support business operations, you need to ensure that those applications don't compromise your network security posture.

Mark Lesswing

Senior Vice President and
Chief Technology Officer
National Association of REALTORS®
mlesswing@crt.realtors.org

REALTOR Secure program resources
<http://www.realtor.org/crtsecure.nsf/pages/resources?OpenDocument>

News articles on application security: <http://www.webappsec.org/>

How to build, design and test the web security www.owasp.org

Application development security concerns:
http://www.phpwact.org/security/web_application_security