
August 2008

Web Security Best Practices

By Vaclav Vincalek

IT security and web security are everyone's business. More and more organizations are taking steps to protect the customers who visit their websites – and protect their own operations from missing opportunities and suffering data theft disasters.

Most companies are generally aware of the rise in cyber crime, data loss and ID theft that plagues businesses and consumers alike. They may be aware of bleak indicators like a recent national survey from CA Canada showed that more than 20 per cent of enterprises reported a loss of private data as a result of security attacks and breaches. Or, that intellectual property losses doubled from 2006 to 2008. And nearly daily reports of security breaches, like the TJX incident where over 45 million credit cards got hacked, point to the damage that can be done in a single attack.

And most CEOs and CFOs understand the harsh consequences of a web security breach: legal bills, crisis management costs, damage to the company's brand and reputation, reduced web traffic corresponding to lower online revenue, regulatory fines, and the cost of rushed after-the-attack security measures.

They also know that good web security publicized properly can lead to higher online revenues from website visitors who aren't worried about their financial information and ID being hacked.

Some companies may want to do something to protect their clients and themselves, but just aren't sure how to do it.

Here are some helpful tips for improving IT security and web security:

1. Make sure you build security into the web development process. When organizations hire web development companies to build a site or application (and even when they do it in-house), security isn't always a priority. But if the web application hasn't been checked beforehand for vulnerabilities, it's a sitting duck as soon as it goes "live".

Industry analysts suggest that just one in 30 websites is safe. Meanwhile, up to 75 per cent of hacker attacks are against the web application layer. With those kinds of odds, it is essential for new websites to be built with the threat in mind.

2. Get a web application firewall. Given that every organization from a mom and pop store to a Fortune 100 company has a website, it's incredible that web application firewalls (also called deep packet inspection firewalls) are not a standard piece of every company's IT security toolkit... yet. They will be. Look into it.

Network firewalls and virus scanners can help to protect your network from hacker attacks. If your organization doesn't have one, get one today. Most organizations are already covered by these items.

But network firewalls and virus scanners are not effective at protecting your website or web application. They won't stop SQL injection type of attacks or cross site scripting tactics that hackers use to "protected" information. For that, you need a web application firewall.

3. Get experts to conduct a web audit scan to check your web application for vulnerabilities. Then fix the issues.

Even if you've got a web application firewall in place, that won't deal with attacks that made it through before you put it up.

The audit should report on the vulnerabilities that are found and see if your web application is compliant with the dozens of regulatory regimes that govern web security. Companies that provide web security audits may be able to provide this report to you directly.

Fix the vulnerabilities. Conducting a web audit that discovered problems and then ignoring the results is like failing a building safety inspection and continuing to run your business out of the condemned property. Doing nothing could make you extremely liable for any security breach.

Next, sweep the website for problems. Even if you have closed off all of the vulnerabilities, you're still in the same position as someone who plugged all the mouse holes in your house but forgot to deal with the family of rodents that already set up house in your kitchen pantry. Have your IT security people check your website for cross site scripts and related problems like sabotage to your database or the possibility that all of the passwords in your network are already compromised.

If you don't have the in-house IT expertise to find the vulnerabilities, fix them and then fix the damage done by the hackers, the company that provided the web security audit should have consultants available to help you fix the problems.

Vaclav Vincalek is the founder and president of [Pacific Coast Information Systems Ltd](#), a leading provider of technology solutions, and its new products division, [Boonbox](#). He is an expert media consultant and speaker on issues related to IT business management, web security, identity management and data storage. He is also the senior correspondent for the [Pacific Coast Informer](#), authors a [blog](#) about technology solutions and is a contributing writer and columnist in publications dealing with the technology industry.

Vaclav can be reached at info@pcis.com