Realtime publishers

Using Cloud Services to Improve Web Security

The Essentials Series

Web Security Services: Delegating Security Responsibility to the Cloud

sponsored by webroot®

Mike Danseglio

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Web Security Services: Delegating Security Responsibility to the Cloud

Few readers need to be told that the Internet is a dangerous place. Anyone in the IT field is aware that viruses, spam, and malicious Web sites exist. Knowledge of these attacks and vulnerabilities was the domain of specialized security gurus just a few years ago. But the need to understand computer security has spread beyond the domain of specialists. Today, even IT end users need to be aware of threats and countermeasures to some degree.

Why does everyone in the company need to understand computer security? Simply put, the attackers have gotten much better, and they get better every day. This is especially true of those conducting Web-based security threats.

Evolving Web Threats

There was a time, not long ago, when browsing the Web was a relatively painless and safe experience. A user simply fired up Internet Explorer, Netscape Navigator, NCSA Mosaic, or any other Web browser, and went to the site of their choice with little concern that their computer would be attacked, let alone compromised, by the visited site.

This perception of a "safe Web" changed rapidly as Internet use exploded in the late 1990s. Web patrons began to experience the pop-up window advertisement explosion. Whatever site they visited, it seemed like at least one new window would open with a dedicated advertisement. But because the ad sales campaigns only profited when those windows were clicked, the ads became more lucrative and deceptive to users. The pop-up windows began to take the appearance of important operating system (OS) messages, compelling less-experienced users to click; the windows would then quick replace the previous message with an advertisement.

Accompanying this pop-up window explosion was the rapid development of installable toolbars and ActiveX controls. Attackers and advertisers realized that installing these components on a user's computer allowed the attackers and advertisers to control more of the system than just the Web browser. In fact, they could make the computer do just about anything—spawn pop-up windows without a Web site open, use a specific home page and search engine, even force Web traffic to go through a specific channel.

The Web browsers and OSs at the time attempted to warn users and get permission from the user before any such installations. These warnings went largely ignored by users and administrators. The result was computers and networks so deeply infected with malware that they frequently required reinstallation from scratch—erasing the hard drive and starting all over again, only to have the now-even-more-clever malware authors re-infect the systems. In extreme cases, the entire network had to be brought down just to control the spread of malware.

The financial impact of these often-innocent-seeming malware outbreaks grew year after year. The 2008 CSI Computer Crime and Security Survey reports that the highest *average loss per respondent* figure was reported in 2001 at $3,149,000 (Source: 2008 CSI Computer Crime and Security Survey, page 16). This scale of financial loss has a very measurable, and very real, business impact, far beyond the home computer that displays an occasional errant pop-up ad. Businesses cannot afford to lose seven figures per year on preventable issues like malware. And this impact is felt throughout the world and across all industries, not just within the scope of this report.

The response was, beginning in 2002, an explosion of the computer security industry. The system defenders quickly outpaced the attackers and brought the situation rapidly into a more manageable space. The reduction in malware outbreaks greatly shrunk the financial opportunities for attackers. Malware authors, even those with semi-respectable business models, changed their tactics (for example, obtaining explicit consent, providing tools for removal) or went out of business. Some were slapped with civil lawsuits and even arrested.

Unfortunately for the rest of the world, malware authors did not completely go away. Although their tactics changed, their overall goal of making money did not. The outbreak of email scams, phishing, pharming, and countless subtle ploys was unleashed on the IT world. The attackers replaced widespread malware infestations by scaling up their more subtle attacks. They realized, correctly, that sending millions of emails costs exactly as much money as sending hundreds of emails. Unfortunately, attackers also realized that the Web is a great place for their attacks.

Today's Web Threats

Many users and IT professionals still surf Web sites with impunity. The list of protective measures is staggering—hardware and software firewalls, virus scanners, browser protection, more vigilant Web site administration, and User Access Control, just to name a few—so how could any malware possibly get to the computer, much less infect it? The reality is that attackers are only concerned with one goal: making money. For as long as there is money to be made by attacking computers, attackers will find a way to do so.

Interestingly, there is even more money available than back in the early days of Internet attacks. Our worldwide economy knows no boundaries. That means an attacker can make just as much profit from a successful attack in North America as she can with success in Asia, Europe, or anywhere else. And the pervasive reach of the Internet enables her to attack any of these places from anywhere in the world. A free Internet connection at a coffee shop in Omaha is just as profitable as a dedicated high-speed link directly into the backbone.

The targets for attack have also evolved. Today, any successful compromise can be profitable. Of course, there are certainly more opportune targets. Attackers tend to gravitate toward companies that may yield information that can be sold (for example, credit card records, competitive data) or used for blackmail (for example, unfiled patents). But the ability of attackers to profit on even the most unexpected or least interesting data should not be underestimated.

Top Two Profitable Data Elements—A Surprising Statistic

Lists of valid credit cards are often sold between attackers. Their value is fairly obvious and doesn't require explanation. But you might not know that the second most valuable piece of data that an attacker can sell is a *World of Warcraft (WoW)* account. For the past several years, attackers have targeted home users and their WoW account information. Per account, they are worth more than 100 times a credit card. This has led to extensive security measures by Blizzard (the publisher of WoW), including two-factor authentication, centralized account auditing, and WoW-specific malware scanners.

Luckily, this type of data is rarely kept on business computers. But you should consider that if data from an online game about Orcs and Elves can be highly profitable, your business data can as well.

A key behavioral change for attackers is the way they exploit computers. In general, attackers seek the weakest security link in a chain to perform their attacks. For example, a user at a corporate desktop receives an email from Facebook that a friend has a new photo, so the user clicks the link and takes a look. There are many actions that happen during that one simple check:

- The link within the email can be a fake (phishing or spear phishing)
- The email can contain a worm disguised as a Facebook link
- The specific Facebook server could be subject to a DNS redirection attack, sending the user to a false server
- The Facebook page could be compromised and hosting a browser-based attack
- The advertisements on Facebook could be compromised and hosting Flash-based attacks

The list of potential attacks for this scenario goes on and on, as do the variants on the scenario. And most of these attacks, including the ones that are most effective today, are Web-based.

Many attackers have followed the trend of users Web surfing at work to compromise these users. They know that social networking sites and services like Facebook, Twitter, and MySpace are frequented by users from the workplace. These sites are also becoming more work-related over time. Many companies use Facebook and Twitter effectively for legitimate corporate communications and building product communities. But these Web sites weren't built around strong security. They were built for social networking. Security flaws should be expected in sites like this. Attackers know this and know that such sites can be a weak link.

Evolving Security Measures

There are many ways to defend against these attacks. Many organizations have deployed large on-site security infrastructures over the past several years. These infrastructures often include malware-scanning software on each computer, centralized firewalls, dedicated email scanners, application-specific malware prevention tools, and more. Some are self-managing while others require centralized operation and monitoring to remain effective. The variety of tools available is virtually limitless, as is the operational cost, effectiveness, and impact on user and IT staff productivity.

Protecting against the dynamic changing attack landscape in the most cost-efficient and seamless manner is the goal of any security solution. This goal is actually achievable with the variety of flexible approaches in the market. But you need to understand the available approaches. Most of them are well-understood and have been around for years. But a newer approach, cloud-based security, has recently emerged and shown the potential to address a number of today's evolving Web-based threats.

Cloud-Based Security Solutions

The idea of cloud computing is not new. Offloading a portion of IT tasks to a service provider is a concept that has been in use for years. This has been especially true for processing large volumes of data or crunching numbers. In recent years, technology has evolved to allow virtually any task to be offloaded in this way. Tasks such as word processing and email can be handled as cloud-based services today where they were inflexible just a short time ago.

Like these other technology services, security is now available as a hostable cloud service. Cloud security approaches are being quickly recognized as a highly-effective defense mechanism. Handling security via cloud-based solutions has a number of benefits:

- Fewer attacks reach the corporate resources, reducing the risk of any security gaps or flaws being exploited
- Reduced time to implement security measures
- Reduced strain on corporate resources (for example, less Web traffic reduces network traffic)
- Constantly updated detection methods that catch even the most current attacks without on-site IT intervention
- Corporate policy enforcement (for example, Web site filtering) implemented by a neutral third party, reducing animosity while enforcing policy and security
- Implementation by well-known security firms that have reputations for trustworthiness

Summary

Web security is a complex problem to address. The ever-changing demands of corporate users don't allow IT professionals to simply turn off Web access, even to sites that are often considered unrelated to work. But IT must still enforce security measures to protect corporate assets. In today's constantly-changing security landscape, this requirement is more of a challenge than ever before.

Cloud-based Web security offers a number of benefits in addressing these challenges. Most of these benefits result in a reduced total cost of ownership (TCO) while maintaining the functionality and flexibility that users demand.