



# Your Website May Be A Gateway For Hackers

By Richard A. Diamond ■ *Stradivarius Associates*

**H**aving a website has become a standard for all broadband related businesses. A typical company uses its website to provide general information about itself to the world, to collect customer research and to sell products online. Like any Main Street merchant, it wants to let the world in, but in doing so, it exposes itself to potential attacks from troublemakers—those out for illegal profit, thrills, or revenge.

As the numbers grow, so do the casualties. The list of well known institutions reported to have had their websites attacked includes the White House, the U.S. Senate, NASA, the Department of Justice, the CIA, The New York Times, Warner Brothers, eBay, Yahoo, a Fox television affiliate and many more. In most of these reported cases, the organization's website wasn't connected to an internal database, so an intruder couldn't get sensitive data. Yet the resulting online vandalism—often pornography, embarrassed the site owners, resulting in a tarnished image, decreased public confidence, and possibly even lost sales. When a website is defaced or taken down, damage occurs even when no valuable data is lost.

## What's vulnerable?

A company's web defenses should be structured with several concerns in mind. One main concern is preventing postings that might cause embarrassment, such as nude pictures, or that might alter information on which the public relies, such as prices. Hackers can pull these stunts by finding exposures in the web server or by exploiting bugs in CGI (Common Gateway Interface) scripts—programs that carry out many of the web page's features.

Another concern is the ability to protect confidential information—e-commerce

transactions, customer data, and company secrets—that are in transit, stored on the web server, or on a database that might be connected to the web server. A third concern is to keep the site up and running by preventing the server from being overloaded or otherwise shut off from users—sometimes known as denial of service (DNS). A final goal is to prevent hackers from creating a phantom site that tricks users into believing that it is the organization's actual site.

## Basic setup

One of the first decisions an organization starting up a website will have to make is who will host the site: the company itself or an Internet Service Provider (ISP). Internal hosting is the more secure option but requires heavy administrative oversight. It is also much more expensive because it requires special software, hardware, and technical staff. For small companies with predominantly informational web pages experts say it is generally more cost-effective to share space on an ISP server with other companies. Website hosting has become more secure and less expensive over the last few years and there are many fine companies that offer these services.

If the company hosts its own website, then it will have sole responsibility for security or for hiring consultants to address security issues. But even if the business out sources the site, experts agree that management should take an ownership interest in how security issues are addressed.

Another preliminary consideration is choosing an operating system. Even if the web server software is well protected, exposures may exist in the underlying operating system. Although many operating systems are used in the Internet world,

Microsoft Windows NT and UNIX dominate. NT's advantage over UNIX is that it is more user-friendly. The focus should be on configuring whichever system is used to make sure that it is secure.

Another issue is whether the server contains any information that the company wouldn't want stolen or known publicly. In theory, a company shouldn't put anything proprietary on the web server, such as its internal accounting information. At a recent Internet conference, however, presenters noted that many firms conducting business-to-business e-commerce have placed their web system software on a server that also holds sensitive data. Since they have not segregated their web systems on separate servers, their internal data remains within easy striking distance of hackers.

Experts also recommend using the web server only for web services, not for other Internet services, such as telnet (which gives users remote control over the computer). Such services can open up avenues of attack.

## Detection tools

To address the potential risks inherent in most websites, the following components are important: forensic devices, firewalls, intrusion detection systems, system vulnerability scanners, and Internet scanners.

Forensic tools. One of the first considerations is protecting the web server from tampering. Forensic products are available that alert the site administrator if anything on the server has been changed by an internal or external user. Such products also detect when accidents or simple corruption alter a protected file or directory.

Firewalls. Much has been written about firewalls, the hardware or software

components that allow only authorized traffic onto a company's internal systems. But should the company's web server be protected by a firewall just as the corporate network is? Or is it only important to secure the public web site from internal systems to ensure that the web does not give hackers a back door into the corporate coffers?

Most corporate sites are also concerned about the integrity of data on the website itself, and they will, therefore, need to place a firewall between the web server and the Internet.

Failing to do so can create numerous exposures, according to Rubin, Geer, and Ranum in the Web Security Sourcebook. For example, web sites that need to be updated frequently require access from the inside by the system administrator. That access constitutes a potential point for a hacker to reach the web server. Also, if the web site itself is not secure, a hacker could gain control of its system and use that access to sneak through the network firewall into the company's internal systems.

Putting a web server inside the firewall enhances security and makes site maintenance much easier; administrators can easily update the site. On the other hand, putting the web inside the firewall may introduce a new problem. As Rubin, Geer, and Ranum write, "if the web server is somehow compromised behind the firewall, it may act as a jumping-off point for attack against the soft underbelly of the network."

The company should also have a robust firewall separating the web from the internal network, experts say. Having the Web server protected by the internal firewall not only helps to keep hackers from the corporate network but also protects the web server from attacks by disgruntled employees who might want to sabotage the web site. Still, firewalls are far from a panacea. Ranum cautions that hackers can disguise their activity as legitimate traffic that the firewall won't filter out.

Intrusion detection. Sites should, therefore, also be protected by an intrusion detection system (IDS). An IDS extends "management capabilities by mon-

itoring activity, examining message packets for patterns of abnormal activity, identifying known electronic attack signatures and misuse, and providing an alert mechanism to bring such problems to your attention in a timely fashion," explains, Paul Lago, CISSP, who is responsible for website security at ImagiNet Communications, Denver, CO.

IDSs can be placed on the web server, on the network, or both. The software is the same, though it may need to be configured differently for each application.

In a usual IDS setup, the IDS's main software runs on the corporate network server, while the "agent" software runs on the web server. The agent can monitor attempted, successful, or undesirable logins and detect "rogue processes" running on the system. Critical to any good host-based IDS is its ability to take corrective action to any attack, such as replace a modified or deleted web page, and notify appropriate personnel with the exact details of what happened.

It is also advisable to have software that is updated regularly with the newest "attack signatures"—or methods of invading websites—used by hackers. Many pieces of IDS software have this update capability built in, though separate pieces of software with that ability are also available.

Vulnerability scanners. System scanners examine the web server in search of vulnerabilities created by misconfiguration. They are used almost as often to examine a corporation's primary network assets. These tools also indicate how the server can be configured to patch the hole and should be run periodically, since security is a fluid process and new vulnerabilities regularly appear.

Among the most common vulnerabilities in corporate websites are bugs in computing language called CGI scripts. As mentioned, CGI scripts are programs written to get the web page to do tasks, such as count the number of visitors.

Some websites, for example, ask for user registration. If the registration script isn't written properly, a hacker can type, say, a string of the letter "x" in the box where the registrant's name is supposed to go. This string can cause what's known

as a "buffer overflow" on the system, meaning more data is sent to a portion of the system called the buffer than it can handle. Buffer overflows can crash programs or, much worse, allow the artful hacker to get system administrator privileges on the server.

Programmers who don't know how to write the scripts securely unwittingly create such bugs. Of course, the best approach is to write secure CGI scripts that prevent such attacks, but scanning can catch a good portion of the holes.

Many organizations have "interactive" websites, enabling surfers to post files, such as bulletin board comments, to the site. This feature also creates a vulnerability through which users can upload malicious code onto the site, wreaking havoc not only on the affected pages but also on other users downloading the code. To counter this threat, experts advise, interactive sites should include software that scans files for problems in real time as they are being uploaded.

Internet scanners. System scanners simply search for vulnerabilities; Internet scanners actually attack the web server in an attempt to break into it. Web site administrators can typically run scanners on their own sites as a preemptive defensive strategy. If the scanner succeeds in finding an entryway, the site administrator knows that the hole must be closed.

### User controls

In addition to protecting the site as a whole from hacker attacks, site administrators must keep authorized surfers out of restricted areas—keeping customers out of each others' records, for example. Administrators may also need to address concerns related to e-commerce, such as verifying the user's identity and securing data in transit. Several tools are available.

Address verification. Site administrators can configure the operating system software to restrict access to specific web data based on the customer's Internet Protocol (IP) address or host name. Some hackers try to trick the server about their true identity—a ploy known as "spoofing." Servers can be configured to check the authenticity of addresses and host names before granting access, but this

strategy is "not considered a strong form of access control. IP address restriction should be combined with a check for user name and password.

Encryption and authentication. One of the biggest impediments to e-commerce has been the fear that sensitive information, such as credit card numbers, will be intercepted in transit. Another concern is that the parties on either end of the transaction are who they purport to be. Encryption and authentication address these concerns, and a website designed to conduct e-commerce must be enabled with these technologies. As the industry has progressed, these security features have been built into some web software, but it has to be properly configured.

### Planning

As is evident from the preceding overview, creating and maintaining a secure website is a challenging and complex task. Planning is crucial, and the process

cannot be rushed. Allowing someone outside of IT to set the website setup schedule is a big mistake. Sales and marketing staff and others often rush the company to put up a site to keep pace with a competitor. In the ensuing setup, security is often shortchanged. Security is most successful when it is built into a web setup from the beginning—yet another example of how good cyberspace security mirrors the principles of traditional physical security.

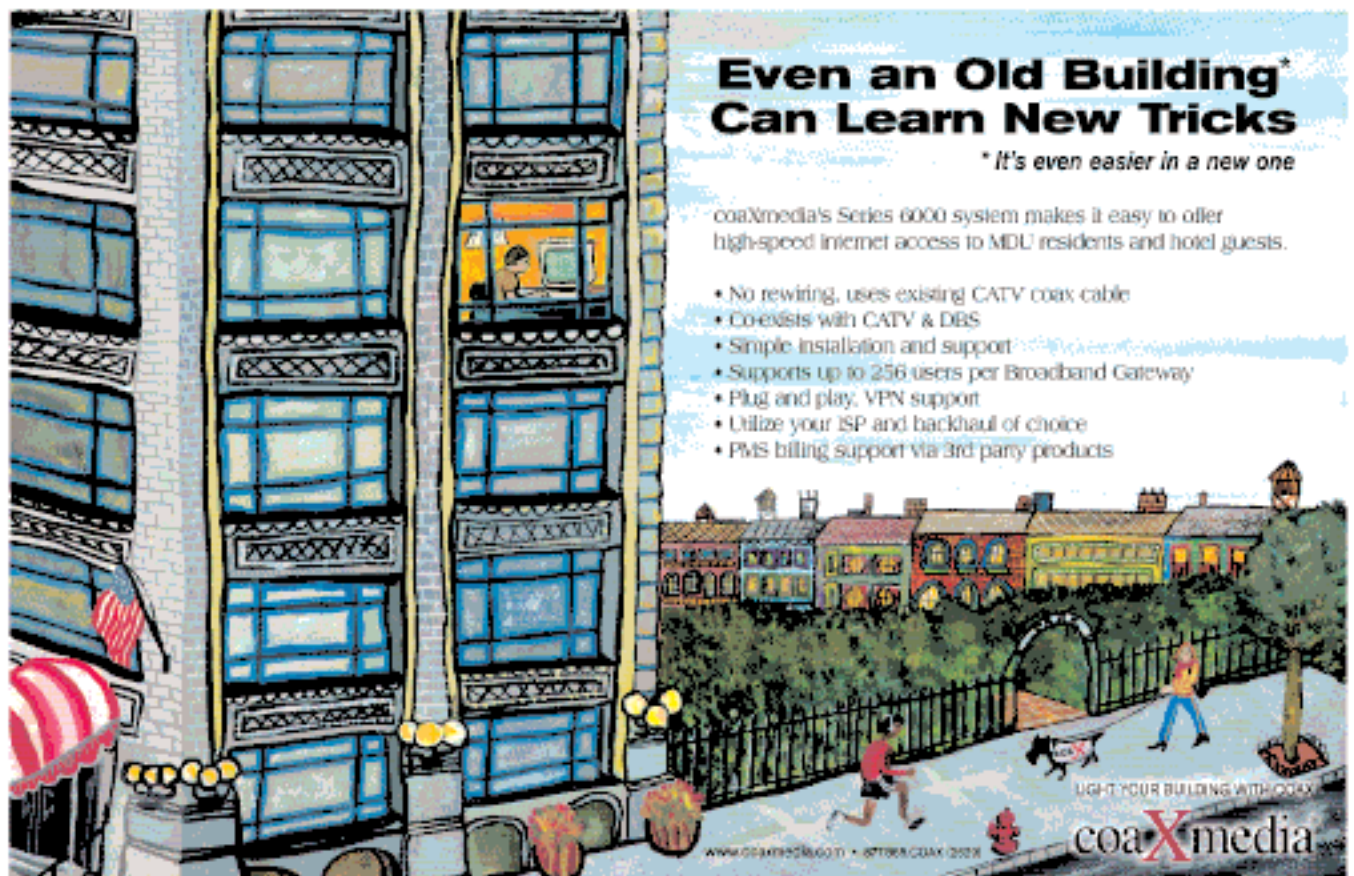
Not every company will have the in-house experience to set up, configure, and secure a web server. Companies may, therefore, want to turn to a contract firm for assistance however, such firms should be interviewed to ensure that they have the expertise claimed.

Many organizations put firewalls and other hardware in place and assume that security is taken care of, but cybersecurity (like physical security) is a dynamic process. It must be continually evaluated and updated. So follow these steps and

make sure that you are protecting your important corporate assets. If you don't, you will always be At Risk. ■

### About the Author

*Richard A. Diamond is the President & CEO of Stradivarius Associates which specializes in business strategy consulting for public and private companies around the world. He actively consults with ImagiNet (www.imagi.net) a leading secure managed network service provider, offering a comprehensive suite of network management, online data backup, WAN and security products and services. ImagiNet has operated its "state of the art" Secure Operations Center 24 x 7 x 365 for over 17 years. He can be reached via email at rdiamond@stradass.com.*



**Even an Old Building\* Can Learn New Tricks**

*\* It's even easier in a new one*

coaXmedia's Series 6000 system makes it easy to offer high-speed Internet access to MDU residents and hotel guests.

- No rewiring, uses existing CATV coax cable
- Co-exists with CATV & DBS
- Simple installation and support
- Supports up to 256 users per Broadband Gateway
- Plug and play, VPN support
- Utilize your ISP and backhaul of choice
- PMS billing support via 3rd party products

LIGHT-UP YOUR BUILDING WITH COAX

coaXmedia

www.coaxmedia.com • 877.668.6001 • 877.668.COAX.2003