The Importance of Improving and Adapting Web Security

With so much depending on Web site availability, CSOs are considering new ways to be cost-effectively proactive and vigilant

In a remarkably short time, websites have become an incalculably valuable part of doing business. They have redefined how enterprises are run—and not only through e-commerce. Companies use Web sites to interact with customers, partners, and suppliers; they are also increasingly shifting mission-critical processes to the Web for better resource allocation and cost efficiency. The business models of some companies—SaaS vendors, cloud service providers, and social media purveyors—are predicated on reliable Web site uptime.

Thanks to these new business models and activities, organizations also have a much broader awareness of how critical Web services are. When a Web site is unavailable—or, worse yet, hacked—there are serious implications. These include everything from disclosure of breaches and liability to extortion and loss of customers and intellectual property.

A recent IDG Research Services survey confirmed that the majority of today's technology and security executives are highly concerned about Web security. The survey defined Web security as "technologies and processes for protecting Web servers and Web users from compromise of data, compromise of systems, and denial of service." Examples included Web application firewalls, DDoS mitigation, and user validation.

There was nearly universal agreement among respondents that Web security is equally important (76 percent) or more important (14 percent) than email or FTP security. The issue is primarily dealt with by IT, which is involved 79 percent of the time, while security is involved only 50 percent of the time.

Of course, Web security isn't the only thing survey respondents are concerned about. Web site availability was mentioned frequently, with malware close behind. Data loss and vandalism were also high on the list.

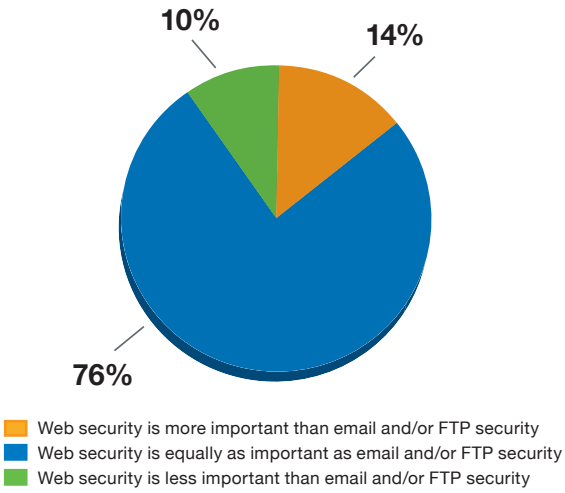
Challenges to Web Security Deployment

Yet despite these widespread concerns, organizations continue to view the cost and reporting capabilities of Web security solutions as major impediments to deployment. A majority of respondents said the cost of security solutions is too high (59 percent) and that current solutions provide inadequate visibility into Web site activity or reporting (51 percent).

At the same time, IT and security executives worry about the limitations of security solutions:

CSO Custom Solutions Group

Prioritization of Web Security vs. Email and FTP Security



SOURCE: IDG Research Services, December 2012

the inability of solutions to scale (30 percent) tops the list, followed by the difficulty of maintaining site availability when a security event occurs (24 percent). They're concerned that Web security solutions demand too much staff time (24 percent), and that their network may lack the processing power to provide the security monitoring necessary during heavy volumes of activity (18 percent).

One big challenge relates to the fact that while enterprises have been forced to employ point solutions for Web security, hackers are becoming more creative. Along with shifting their attacks from the network layer to the application layer, hackers are using different attacks in conjunction with each other. For instance, to cover the evidence of attacking an application through what's known as a SQL injection attack, hackers will launch a DDoS attack as a distraction, the same way a thief might set a fire to conceal evidence of the actual crime.

Another problem is user validation, which relates to Web application firewalls. To get around the problem of a lack of IPv4 IP addresses, a company might set up one server with one IP address as a virtual proxy server, giving other users virtual addresses. This concept works fine until a hacker walks into an Internet cafe, gets a virtual IP address, and launches an attack using the temporary addresses. How can a Web security solution validate whether a user request is coming from a hacker or from someone legitimately using a proxy?

Options for Web Security Deployment

How indeed? Given their internal limitations and the importance of Web security, it's no surprise that an increasing number of companies are considering cloud-based Web security that focuses on providing an "always-on" capability. This concept is already taking hold among the IDG Research survey respondents: just over one-quarter of organizations have these types of solutions in place, with an additional three-fifths of organizations likely to consider them.

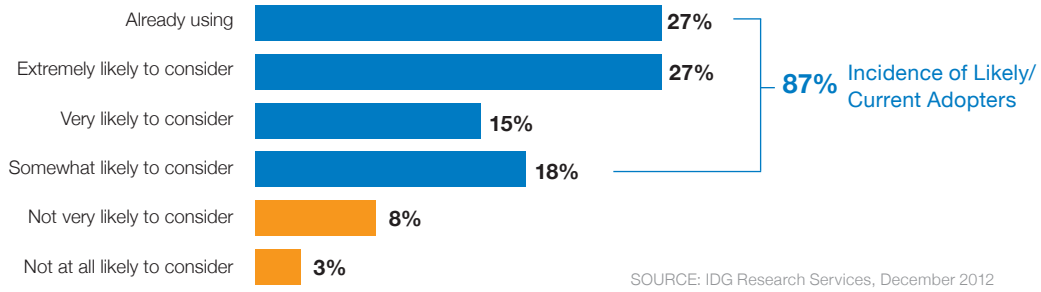
The survey respondents expect a number of specific benefits from their security capabilities, including the ability to be proactive about security, increase vigilance, and deploy high-performing solutions in place of point solutions. At the same time, they'd like those capabilities to help them decrease costs and ease maintenance concerns—hence the interest in cloud-based Web security among today's enterprises.

Part of the potential cost savings stems from the ability to shift security investments from a capital to an operational expense model. Deploying a security appliance such as a Web application firewall requires procurement, installation, licensing, training, and upgrading.

What's more, there's the question of scalability with an on-premise solution. It's extremely difficult for IT to gauge the extent of an attack on one of its servers, not to mention the impact an attack might have on the network.

Akamai specializes in providing cloud-based Web security through its Akamai Intelligent

Adoption of "Always-On" Web Security Solutions



SOURCE: IDG Research Services, December 2012

Platform. The platform offloads attack mitigation and automatically incorporates scalability through a globally distributed network of appliances and software that can be positioned on the edge of an enterprise's network. There they act as checkpoints for attacks, deflecting them before they compromise an enterprise's network, servers, or data center.

"We offer a cloud-based Web security solution that always operates in-line, features on-demand scalability, is globally distributed, and is targeted at medium-sized to large enterprises," says Akamai's Vice President of Security Products, John Summers. "Most other solutions fall short in scalability and target small to medium-sized businesses, or offer just point solutions. Enterprises need all four components of Web security—DDoS mitigation (network and application layer), user validation, Domain Name System (DNS) security, and Web application security—working together."

Akamai's capabilities mean enterprises can forego dealing with point solutions and take advantage of monitoring that addresses those four key components of Web security. At the same time, a cloud-based solution means that costs shift from capital to operational budgets, making them highly predictable on a month-over-month basis.

By providing an integrated solution that maintains Web security and protects the enterprise's Web-related activities from attack and distress, Akamai can deliver relief to those who manage security as well as those who pay for it. ■

For more information, visit **www.akamai.com**.