Improving Web Application Security

With employees and customers increasingly depending on corporate Websites, reliability and security have become more critical than ever.

**THE WEB IS AN INDISPENSIBLE MEANS OF COMMUNICATION BETWEEN THE ENTERPRISE AND ITS CUSTOMERS, SUPPLIERS, PARTNERS AND EMPLOYEES. A RECENT IDG RESEARCH SURVEY FOUND THAT, ON AVERAGE, ENTERPRISE DATA CENTERS HOST 39 DISCRETE WEB APPLICATIONS FOR SUCH COMMUNICATION.**

For both customers and employees, it’s crucial that these applications are both reliable and secure. Unfortunately, the same survey shows that companies find themselves under frequent attack and these attacks increasingly threaten productivity, reliability and reputation. IT professionals fear that the problem will get worse before it gets better, impacting their ability to serve both these groups, maintain reliability and reduce costs.

So what kind of Web application security should companies use to protect themselves from the dangers of downtime, data loss and negative brand perception? The options are complex, because there are so many permutations: appliances, firewalls, cloud-based security. But as daunting as it may appear to sift through both the problems of Web application security and the number of solutions, there are ways enterprises can mitigate their challenges.

**CONCERN ABOUT WEB APPLICATION SECURITY**

The survey results—from 106 security decision-makers, more than 60 percent of whom are at companies with more than 1,000 employees—are sobering. More than half reported that their Web applications are subjected to threats on a daily basis, whereas some 78 percent reported that they are exposed to threats at least once a week.

The problem, as Daniel Shugrue, senior product marketing manager at Akamai Technologies, noted in his blog earlier this year, is that Web applications are “fraught with vulnerabilities. … 95 percent of malware infections in 2011 occurred through Web applications [because] apps are being built without proper vulnerability testing.”

Even more alarming, the trend is worsening. More than 70 percent of the respondents reported that the volume of Web application threats they experience today has increased compared to 18 months ago. An even higher percentage—80 percent—expect Web application threats to increase over the next 18 months.

IT professionals are highly concerned. Some 43 percent worry about application performance issues as well as the time and trouble incurred in “IT fire drills”—the scramble that occurs when a threat appears suddenly and everyone’s attention...
“Web applications are fraught with vulnerabilities... 95 percent of malware infections in 2011 occurred through Web applications [because] apps are being built without proper vulnerability testing.”

is focused on it (see chart below).

At the same time, 39 percent reported that dealing with such threats increases their operational costs. At least three-quarters consider it necessary to avoid negative results, which they define as either application downtime or a loss of corporate or customer data.

One of the most insidious aspects of these threats is the effect on Website visitors. IT recognizes that an attack is taking place, but visitors only experience poor performance. Without knowing the mitigating factors, visitors can only conclude that a Website doesn’t serve their needs. Employees may complain to IT, which is problematic enough, but potential customers are likely to move on to a competitive site without even registering a complaint—and without coming back.

**Tackling the Web Application Security Challenge**

Although organizations may have become more adept at securing their Web applications from breaches, they’ve been less successful at preventing performance problems or downtime. For these latter issues, companies have a variety of options to choose from in Web application security, each providing varying degrees of success.

Some are using on-premises firewalls, basically appliance-based systems. Enterprise IT managers prefer having a solution within their network, but this requires human intervention at the time of the attack (which may not come fast enough) as well as enough appliances to scale up during an attack without degrading network performance. These appliances also require more capital outlay and operational expense outlay.

Others use a technology—often provided by their ISPs—known as scrubbing, which reroutes traffic when a site is under attack, separating the threat from legitimate traffic. This method tends to focus on network traffic and can leave Web applications vulnerable to common attacks such as SQL injections and cross-site scripting (XSS), both of which exploit security application vulnerabilities to gain access to data.

Companies are also turning to always-on security in the cloud, using a completely off-premises firewall to protect Web applications and guard against distributed-denial-of-service (DDoS) attacks. Such a system detects and deflects threats in HTTP and HTTPS traffic, identifying threats closer to their source and farther from client data centers. Because these firewalls are deployed at the edge of the network rather than in the host data center, they are able to identify and mitigate suspicious traffic without compromising performance.

**How Akamai Helps**

Akamai has years of experience in helping companies improve their customers’ and employees’ Web experiences. Kona Site Defender, Akamai’s flagship security solution, incorporates a Web application firewall that protects global enterprises from Website attacks. It adds an extra layer of security to existing security solutions, so companies can incorporate it into current security deployments.

From a technical standpoint, Akamai’s always-on tools can scale instantly to handle spikes in malicious traffic. Because the firewall capabilities are off-premises, companies can protect their network, their application performance and their reputation by keeping threats outside their perimeter.

From a business standpoint, these solutions offer economical options. Because they are cloud-based, companies pay for them out of operational rather than capital expenses. These solutions also help contain other security costs, because they deliver significantly enhanced protection without requiring investment in new IT security infrastructure.

**Learn more** about Akamai’s Web application security solutions. Visit [akamai.com/security](http://akamai.com/security).