Overcoming the Big Disconnect in Web Security

COMPANIES KNOW HACKERS ARE TARGETING THEM, BUT TOO FEW HAVE PLANS IN PLACE FOR FIGHTING BACK.

DESPITE SIGNIFICANT INVESTMENT IN TIME AND RESOURCES, many companies still are not prepared to deal with potential security problems. A *CSO* survey shows that, even after years of warnings and high-profile breaches, 42 percent of respondents state that while they are not aware of any attacks recently, they can't be certain their organization has not been attacked. Only 28 percent are certain that their organization's Web security has not been compromised recently.

Even more discouraging, 42 percent of respondents do not have an escalation plan in place to combat distributed denial-of-service (DDoS) attacks or data breaches—two security issues that are becoming increasingly common. This is not to say that companies are indifferent to the importance of security. Respondents are well aware that such attacks translate into downtime and data theft, and that has a deleterious effect on a variety of issues: revenue, reputation, and—worst of all—customer experience.

It appears that a disconnect exists between concern and preparation. Companies don't think they're immune to security breaches, but they have yet to determine the best path to reduce risk. The question, then, is: What's the best way to eliminate this disconnect?

What Organizations Know about Web Security

The good news: large enterprises know Web security is a problem. Those with more than 10,000 employees are most likely to state with certainty that they have been attacked recently. The majority of small companies, those with fewer than 1,000 employees, are uncertain or don't know, according to the *CSO* survey. Large companies are also more likely than small companies to be concerned with protecting all of their computing assets rather than the data in one or two key applications.

More good news: companies know where many of their vulnerabilities are. Network infrastructure tops the list of assets respondents are most concerned about protecting, followed by email and other non-Web applications, their data center, the Web applications deployed in the data center, their DNS infrastructure, and their cloud applications.

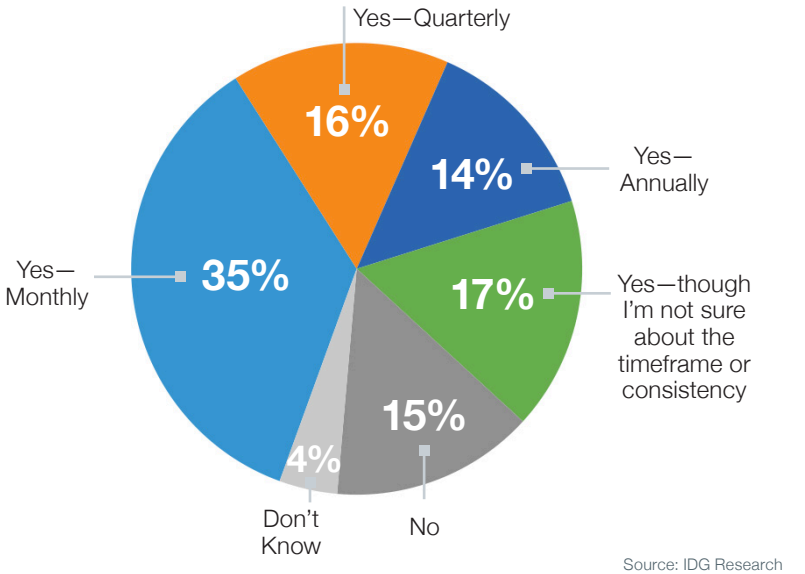
It's encouraging that companies appear to be addressing a wide swath of systems. Taking a holistic view is important, because it means they tend to apply consistent methods to security across the company. Point solutions and piece-meal security leave the potential for gaps and errors, and they increase resource demands when it comes to training and licensing.

What Organizations Are Doing about Security

The survey results are less encouraging in terms of what companies are doing about security. Many of the security disconnects occur here. As noted previously, while the majority of organizations have an escalation plan to combat future DDoS attacks or data breaches, a sizable portion has no such plan in place. This represents one of the biggest security disconnects—the knowledge that there's a problem, but the lack of a response plan in place to remediate it.

CSO
Strategic Marketing Services

OCCURRENCE OF WEB VULNERABILITY SCANS



Source: IDG Research

Also troubling is the frequency with which companies perform Web vulnerability scans to determine potential trouble spots. Among survey respondents, almost half—45 percent—indicate they perform this important activity less frequently than every month: 16 percent say quarterly, 14 percent say annually, and 15 percent say not at all. Large companies (more than 10,000 employees) are more likely than midmarket companies (1,000 to 9,999 employees) to conduct Web vulnerability scans on a regular (that is, monthly) basis. They're also more likely to have an escalation plan in place should problems arise. But because the threat landscape shifts constantly—no one can be sure where a breach or attack might begin—protection requires paying closer attention to this issue.

What Worries Organizations Most about Web Security

This is not to say that companies aren't concerned about Web security. On average, respondents understand that extended site or application downtime has a significant impact. Worse, the impact is spread across multiple aspects of the company, because it can affect customer satisfaction (which can impact revenues), brand reputation (which can affect revenue and stock price), and the ability to do business (which can impact employee productivity).

Too many times, organizations have seen the impact that downtime can have, especially when it comes to both costs and revenue. The Ponemon Institute, which focuses on security-related issues, reports that the average cost per minute of unplanned downtime rose from $5,600 in 2010 to $7,900 in 2013.[1] Ponemon also notes in its *2014 Cost of Data Breach Study: Global Analysis* that the average cost of downtime is $3.5 million in U.S. dollars—15 percent more than what it cost last year.

These numbers force the question: Why are companies willing to live with security concerns? The answers are simple. Sometimes companies lack the resources to focus on security. As security gets more complex, it becomes harder to find the staff to address it—and the budget to tackle its vagaries. At the same time, as hackers grow more sophisticated in their methods, it becomes harder for companies to keep up. With this escalation, companies may not know exactly where they are most vulnerable, or the most cost-effective way to tackle the problem.

How to Eliminate the Disconnect

The question of eliminating these disconnects thus moves front and center. If organizations don't have the expertise or the resources to devote to security, the time has come for them to think about partnering with someone who does, someone for whom security is a core competency.

Partnering with a security service provider is an effective way to tackle many of the security issues enterprises face. Security service providers have the necessary resources. They have the staff to focus on all facets of security and systems. They can provide companies with a way to keep up with the shifting threat landscape—one that the provider evolves over time, rather than forcing companies to constantly upgrade their security solutions.

Moving Web security solutions to the cloud is an increasing trend. Akamai cloud security solutions provide both significant experience and deep security intelligence in protecting websites by incorporating Web application firewalls, DDoS defense, and DNS resolution. Partnering with a security provider like Akamai enables organizations to focus on their business priorities without letting concerns about security grow so large they become overwhelming.

[1] www.datacenter-knowledge.com/archives/2013/12/03/study-cost-data-center-downtime-rising/

For more information about Akamai security services, go to **www.akamai.com/security**