Enterprise Web Application Security Challenges and Priorities

The importance of web application security is well understood and widely regarded to be of critical importance for the enterprise. These are the results of a recent IDG Research Services survey, which offers insights into the major challenges and priorities of application security in large enterprises in the United States, the United Kingdom, and Hong Kong/Singapore.

Most of the respondents recognize that application security is critical or highly important to both their IT security strategy (83 percent) and their overall IT strategy (82 percent). The research shows that besides firewalls and IPS platforms, which are foundational web application security solutions, other core element are needed to deploy a complete, end-to-end web application security solution, and it goes on to identify these elements.

For the survey, IDG defined application security as the use of software, hardware, and procedural metrics to protect applications—including email—from external threats. Of the 250 enterprise IT executives surveyed, 100 were from the US and the UK, respectively, and 50 hailed from Hong Kong or Singapore. The average size of the companies surveyed was 22,974 employees, and all respondents were from organizations with at least 500 employees.

The survey not only sheds light on the status of web application security—illuminating its most significant challenges and illustrating its underlying components—but it also gives a glimpse into how IT leaders plan to invest in technology that addresses current vulnerabilities.

**End-to-end application security**

What does end-to-end really mean when it comes to application security? To better understand what it entails, the executives were asked to identify the elements that constitute a complete, end-to-end application security solution.

Firewalls, web application vulnerability scanning, and intrusion prevention system (IPS) platforms were the top requirements. Firewalls are the top element in every geography, reinforcing the demand for firewalls as a cornerstone of web application security. But the survey found some regional differences. For example, executives in the US feel more strongly about including HTTPS/SSL offloading in a complete web application security solution than do executives in the UK or Hong Kong/Singapore.

**Top challenges for ensuring web application security**

When asked to identify the top three challenges for ensuring that their organization’s internal and external web applications aren’t compromised by attackers, a third of the executives pointed to securing cloud-based applications as their top
concern. This was followed closely by securing legacy/older applications (32 percent) and mobile applications (30 percent).

But some regional differences emerged, with 48 percent of the Hong King/Singapore executives citing securing cloud-based applications as their top challenge, compared to 30 percent in the US and 29 percent in the UK. This perhaps suggests that executives in the latter markets are more comfortable with their existing security infrastructure. Interestingly, executives in the US are most challenged by a lack of application security skills and methods.

Hong King/Singapore IT executives also viewed scalability of security solutions as a significantly larger concern than did US and UK respondents, suggesting a more urgent need for secure, fast-growing web applications in these Asian markets.

Some differences in viewpoints stemmed from the size of the company surveyed. For example, respondents from larger companies, those with 10,000+ employees, were more likely than those from smaller companies to report policy generation and management as a top challenge. Whereas smaller enterprises are more accustomed to ad hoc management processes, larger companies show greater interest in best practices and more-disciplined security management approaches built around established policies.

**Identifying the weakest points in the application security infrastructure**

Executives view legacy applications and mobile apps as the weakest points in the application infrastructure. The dichotomy between these two distinct technology arenas indicates the ongoing IT challenge of securing existing applications while coping with the rapidly increasing need to secure new mobile applications.

The research found that those with director or VP titles are more likely than those with C-level titles to report third-party applications as the weakest point in the application infrastructure.
Hong Kong/Singapore were most likely to identify cloud-based and outsourced applications as their infrastructure’s weak points. These markets generally tend to have less legacy technology in place, so legacy applications are the least likely to be considered a weak point.

Budget implications
Financial concerns are always a major factor in selecting web application security solutions. But when budget is not an issue, the top technology in application security slated for investment over the next six months is IPS, cited by 53 percent of the respondents. This was followed by database security (45 percent), with distributed denial of service (DDoS) protection and web application firewalls tied for third (44 percent).

IPS is the technology that respondents would be most likely to invest in to address application security vulnerabilities. Although mentioned by only a small percentage in the other markets, web caching stands out in the UK as an attractive potential investment, perhaps because of regional demands for reducing network bandwidth utilization and increasing web application performance.

Conclusions
Firewalls and IPS platforms remain the hallmark for web application security, but web application vulnerability scanning, intrusion prevention, advanced threat protection, DDoS protection, email security, and database monitoring are also universally recognized as crucial elements for web application security.

Deploying these elements to complement foundational firewall and IPS platforms enables organizations to successfully implement an end-to-end web application security solution. The enterprise can augment firewalls and IPS platforms to successfully plug any potential security gaps and address issues such as zero-day protection and DDoS prevention.

Although the research found some regional differences and viewpoints that varied with company size, all the organizations show a need for end-to-end application security solutions that thoroughly protect enterprise resources.

The market-leading family of FortiGate Enterprise Firewalls, Unified Threat Management (UTM), and Data Center Application Security Appliances delivers advanced protection from sophisticated threats while simplifying IT infrastructure. Fortinet’s diverse product line of complementary solutions enables businesses and government organizations to consolidate stand-alone products, embrace new technologies, and implement innovative business initiatives with assurance that the network, applications, and data—extending out to every endpoint—are totally secure.

For more information, visit www.fortinet.com