

Enforcing Web Application Security in the E-Commerce Enterprise

A Growing Industry, a Growing Threat

The growth of e-commerce since the 1990's has been remarkable, with sales reaching an estimated \$45.5 billion in the U.S. in 2002 according to the Department of Commerce. But while the numbers of online shoppers and sales are expected to increase in coming years, privacy and security concerns are still seen as a major impediment to growth. According to The UCLA Internet Report, "Surveying the Digital Future," an authoritative annual study of online activity, more than 88% of adult respondents in 2002 expressed concerns about the privacy of their personal information when shopping on the Internet. And in what the survey authors termed a "continuing major problem," apprehension about credit card security on the Internet remained as high as ever, with 92.4% of adult respondents expressing worries about the safety of their credit card information online. The number one reason cited for these fears? Hackers.

Hacking and Liability

According to the CERT Coordination Center, a leading authority on Internet security, hacking is growing exponentially. From 2000 to 2002, reported incidents rose from 21,756 to 82,094, and if current levels continue, 2003 will see more than 150,000 hacking incidents. Adding to e-commerce security concerns is the rising tide of identity theft crimes, which are now the leading source of consumer complaints registered with the Federal Trade Commission. The numbers add up to a sobering reality: cybercrime is a fundamental threat to e-commerce firms, not just in terms of injury to individual customers but in terms of potentially devastating lawsuits, government fines or long-lasting damage to your brand. As a matter of sound business, it is essential for online retailers to prevent malicious attacks on the databases that store and track transactions and the web applications used to process them. Unfortunately for the industry, the application layer has long been the most vulnerable element in the e-commerce IT infrastructure.

Web Applications: the Weakest Link

Highly vulnerable to malicious hackers, web applications provide an entry point through which credit card numbers and other sensitive data can be accessed and stolen. This vulnerability is present because current security solutions—including network firewalls, intrusion detection systems and encryption, and manual measures such as aggressive quality assurance and audit procedures—are incapable of preventing attacks at the application layer. Applications provide hackers with the opportunity to use SQL injection techniques to gain access to tables in backend databases, thereby gaining access to sensitive customer data. In addition, viruses such as Nimda and Code Red, both of which infect systems the application layer, can take down a site for days at a time and do irreparable damage to a company's reputation.

- Gartner estimates that 80% of all corporate hacks are now targeted specifically at web applications.
- A flaw in the Microsoft Password application that enabled hackers to steal private information and credit card numbers exposed the software giant to potential government fines of up to \$2.2 trillion.
- The UCLA Internet Report – Year Three found that 54.3% of people surveyed said they are very concerned or extremely concerned about the privacy of their personal information when buying online.

“Computer security... is being driven not only by companies' need to protect themselves from the explicit damage a hacking incident or other security violation may cause but also by potential liability — regulatory, contractual, or criminal.”

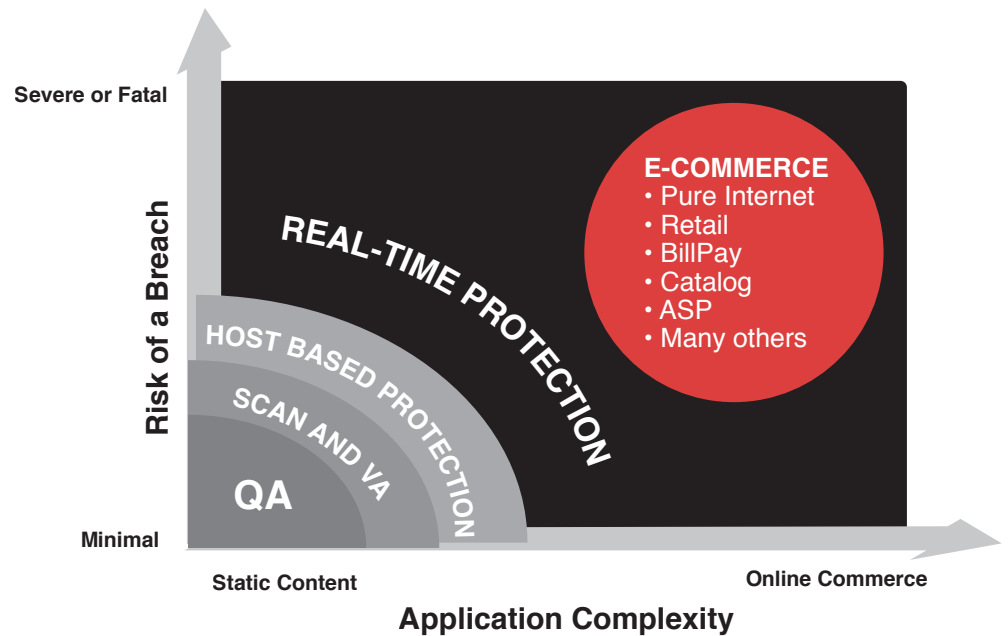
Specific Protection for E-Commerce

A critical component within the layered security architecture of the financial services enterprise, the Teros-100 APS blocks both known and undocumented web application attacks in real-time. It also has an intelligent learning engine that enables the development of application-specific security policies—a vital capability in today's disparate, multi-platform computing environments. Deployed behind the firewall and in front of the web server, the Teros-100:

- Monitors, filters and analyzes both incoming and outgoing HTTP packets in the data stream
- Uses a comprehensive rule set to detect suspicious activity
- Blocks all 16 major categories of web application attack
- Effectively prevents credit card and social security number theft
- Helps ensure compliance with Sarbanes-Oxley, the Patriot Act, HIPAA, Gramm-Leach-Bliley, the Database Breach Notification Act and other legislation

The Teros Web Application Security Solution

Teros reduces web application vulnerability to zero with a hardened appliance and innovative security technology that provide 100% protection against web-based attacks. Plugging a major security gap that cannot be addressed by firewalls, intrusion detection systems and other network-centric strategies, the Teros-100 APS enables organizations to proactively enforce stringent security and privacy strategies, and specifically prevent SQL injection and database-specific attacks. By guarding web applications against hackers, Teros protects your customers from identity theft and financial fraud while shielding your brand from site defacements and downtime. **There is no stronger technology for securing your online business operations and preserving the trust of your customers!**



The data exchanged during e-commerce between customers, businesses and ASPs includes sensitive customer information such as identification, account numbers, personal financial data, employment history and more. A breach of security would result in enormous penalties and reputation damage to the e-commerce provider. The success of any and all e-commerce initiatives lies in convincing constituents, first and foremost, that their data is secure and will remain confidential.

Contacting Teros

The Teros-100 APS is available immediately from Teros and its business partners worldwide. To contact Teros please call 800-TEROS99, visit our website (www.teros.com), or write to us at info@teros.com.