

Enforcing Web Application Security for Government

Better Public Services, but Increased Security Threats

Just as the Internet has revolutionized the way individuals and organizations communicate, channel information and conduct transactions at home and at the workplace, so has it changed our interactions with government. Through e-mail and the Web, elected representatives have become more accessible, and citizens have come to expect round-the-clock access to economic statistics, road safety reports, school lunch menus and tax information. But while online businesses must concern themselves with privacy and security from an economic or business standpoint, for government entities maintaining constituent privacy and preventing security breaches are paramount concerns. This is especially true in a world threatened by terrorism.

A Prime Target

Government websites and databases have long been favorite targets of hackers, both because of the value of the information contained within and the prestige of breaking into the cyber equivalent of Fort Knox. A long list of government agencies have been hacked over the years, from various branches of the military and the Treasury Department to NASA, the National Institutes of Health and the federal court system. The response to the growing threat of malicious attacks in the private and public spheres has been increased regulation and stringent new legislative measures, including HIPAA, Gramm-Leach-Bliley and the Patriot Act. With the implementation of California law SB 1386 in July 2003, however, the stakes for government officials have been raised considerably.

Web Applications: the Weakest Link

California's SB 1386, which applies to any state agency or private enterprise doing business in California, whether based in the state or not, requires that unauthorized database intrusions be publicly disclosed. Failure to do so could result in serious liability through class action suits and civil damages. Significantly, the California law, which served as blueprint for the pending federal Database Security Breach Notification Act, was prompted by a hacking intrusion into the state's payroll database. This attack was an ominous event for any government agency that maintains sensitive databases and an online presence. The reason is that 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 web application layer. And as government agencies make more services available online, so grows the threat to both personal privacy and national security.

- According to the Federal Trade Commission, more than 160,000 identity theft complaints were reported in 2001, making it the number one source of consumer complaints in the United States.
- From 2000 to 2002 hacking incidents reported to the CERT Coordination Center, a leading authority on Internet security, rose from 21,756 to 82,094, and if current levels continue, that number will rise to more than 150,000 in 2003.
- California state law SB 1386 for the first time requires that businesses and government agencies must report security breaches.

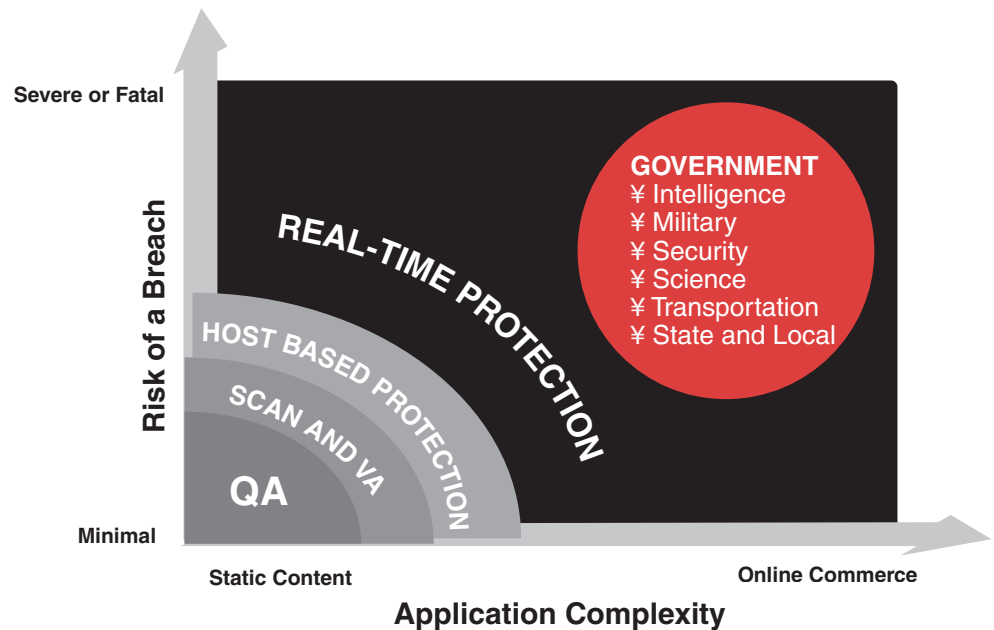
Smart Security to Block Known and Unknown Threats

A critical component within the layered security architecture of the government enterprise, the Teros Gateway 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

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

The Teros Secure Application Gateway

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 Gateway 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 individual citizens from identity theft while protecting the security and reputation of the organization. There is no stronger technology for securing online operations and preserving the public trust.



In an e-government setting, intrusiveness and constituent privacy perception are prime considerations. Most matters in which constituents interact with the government consist of the exchange of extremely sensitive data (name, address, date of birth, social security number, driver's license number, medical records, employment history, criminal record, educational transcripts, financial information, etc.) that can cause a lot of damage if it falls into the wrong hands. The success of any and all e-government initiatives lies in convincing constituents, first and foremost, that their data is secure and will remain confidential. Then, and only then, will constituents feel comfortable enough to support, use and champion e-government initiatives.

Contacting Teros

The Teros Gateway is available immediately from Teros and its business partners worldwide. To contact Teros please call 866-TEROS99, visit our website (www.teros.com), or write to us at info@teros.com.