

Government knowledge workers can strengthen cyber-security in 3 ways

From Page 1

number of vulnerability points.

In 2008, Homeland Security Presidential Directive 23 (HSPD-23) responded to this rise in cyber-security incidents by prescribing an array of practices and preventive measures, but budget limitations and competing priorities have inevitably slowed compliance. Recent Government Accountability Office (GAO) testimony before the House of Representatives claimed that 23 of 24 major federal agencies fail to consistently apply and enforce authorization practices that would protect data and control access to government IT systems. It is clear that awareness, education and cyber-security solutions need to catch up with existing policy and directives.

Cyber-security cannot be approached as something IT professionals simply handle for an organization -- not given the way the Internet has evolved into a major part of daily professional and personal life. Attack sophistication today is far ahead of where it was only five years ago. As network protection has advanced to counter the threat, the threat has shifted from the system to the user, and the user (who is accustomed to ubiquitous connectivity) has become an easier target for exploitation.

Knowledge workers in the government and elsewhere need to recognize that they are the first line of cyber-security defense. Government must jump-start federal cyber-security efforts in order to provide a starting point for staff education, the protection of sensitive information and the safeguarding of government infrastructures from emerging threats and risks.

No matter the agency or mission, there are three keys to successful government cyber-security efforts:

1. Malware discovery and comprehensive malware awareness

Malware -- small, sophisticated programs that users unknowingly download to their systems -- can compromise proprietary and confidential information, degrade system performance or even hijack a system for criminal purposes. Government and industry must work together to deliver and provide solutions that can detect malware and mitigate it before it causes any security breach. Cyber intelligence can do this by taking

the battle to the threat rather than waiting for the attack. This approach combines proactive and predictive measures for the best results, enabling an organization to see a threat coming well before it arrives. Comprehensive malware discovery and awareness can provide insight into new ways to defend against emerging threats.

2. Education of the knowledge worker

Key steps toward effective, comprehensive cyber-security and malware protection are awareness and education.

Government knowledge workers have become favorite targets of social engineering cyber attacks. To be an effective front line of defense, government employees must understand the basics of how the Internet works, as well as the inherent vulnerabilities and weaknesses of the agency's system and its users. They must understand how malware works and recognize their responsibility in protecting

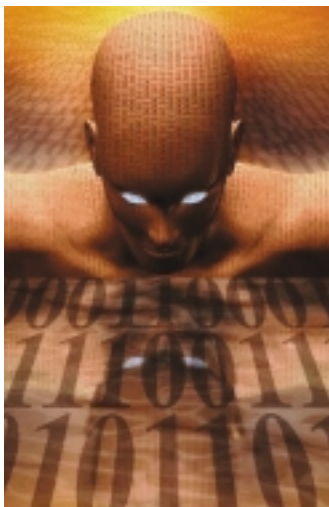
government systems from it.

3. Understanding the risk

With a laptop and a connection to the Internet, cyber-attackers anywhere in the world can investigate and compromise an agency. Their costs are low and the damage they inflict can be devastating. Government must understand this risk and its particular vulnerabilities. With this understanding, an agency can take protective steps that will enable it to continue its mission, even under cyber-attack. There are numerous solutions available on the commercial market, and industry has a role in bringing these solutions to their government customers. The key, however, is determining which commercial solution translates well to government agencies.

HSPD-23 will certainly improve the federal cyber-security landscape, but only if compliance is substantive and not merely formal. By expanding cyber-education, encouraging best practices, and developing leap-ahead security strategies, government and industry will be better positioned to undermine and deter the bad actors operating on the Internet. ■

Mary Craft is senior vice president, national systems, in QinetiQ North America's Mission Solutions Group, and leads QinetiQ North America's cyber-security and operations efforts. She can be reached at: Mary.Craft@QinetiQ-na.com



Blue Ridge CEO describes impact of cyber-theft in GSN video interview

"According to a Symantec spokesperson, cyber-theft is now a more lucrative business than drug trafficking."

This startling statement was made by Mike Fumai, the President and CEO of Blue Ridge Networks, in a video interview in which he described the dire consequences of malware attacks on governments, businesses and consumers.

The interview was conducted by GSN: Government Security News on the day after Blue Ridge took home the winner's trophy in the "Best Anti-Malware Category" of the GSN 2009 Homeland Security Awards Program. The interview is available for viewing on the GSN Video Center at www.gsnmagazine.com/cms/general/2876.html.

In other examples of the impact of malware, Fumai pointed out that the Melissa Hathaway/CSIS Report commissioned by President Obama concluded that \$1 trillion worth of U.S. intellectual property was stolen by cyber-espionage in 2008. He added that cyber-criminals are presently stealing over \$1 million per day from small businesses.

"This stealing impacts everyone," said Fumai. "You can pick up a newspaper every single day reporting of the stealing of identities from consumers or drawing money out of the bank accounts of small businesses. Small businesses that lose \$75,000 or \$150,000 from their bank accounts can be brought to their knees. They're closing their doors every day."

Blue Ridge Networks was named the winner in the GSN 2009 Awards for its AppGuard anti-malware solution, which the



company claims "protects PCs from attack by the latest generation of sophisticated malware threats, increasing endpoint security coverage to address more than 90% of known and unknown vulnerabilities."

According to Fumai, the contemporary malware threats can only be stopped by traditional anti-virus products 20 to 30 percent of the time, because they rely on known malware signatures. Cyber-criminals today are changing their signatures every 10 minutes, he said.

In 10 years of business, said Fumai, Blue Ridge has had zero reported vulnerabilities. ■

Finjan's Malicious Code Research Center (MCRC) finds malware on 77 different government domains

Traditional Web security solutions continue to rely on matching malicious code to a known signature or URL to a database of URLs by categories, and were not designed to prevent today's Web attacks, according to Finjan, Inc., of San Jose, CA, a finalist in GSN's 2009 Homeland Security Awards.

Today, the company asserts, up to 90 percent of malicious code on the Web resides on infected legitimate Web sites, and is typically obfuscated to evade traditional security solutions.

Finjan is the creator of the

Malicious Code Research Center (MCRC), which in the last year has identified malware residing on 77 government domains (.gov) in the U.S., UK and other countries. Finjan alerted the countries to the breaches, enabling them to correct and repair the breaches before they became known to the public.

The company's Secure Web Gateway solutions use patented, active, real-time inspection technologies, by which the code embedded within Web content or files is analyzed and its intentions are understood in real-time, regardless