Government Executive

Need to Know Memo

Cybersecurity

The latest in arming critical networks against hackers.

By Adam Stone

It would be hard to imagine a scenario in which cybersecurity is *not* a pressing government priority.

Activist hackers invade government networks to get their message across, while federal employers are probing their operations—even peering into their workers' communications—in search of breaches. New technologies emerge every day in the battle to bolster security.

Software solutions provider Deltek estimates the federal government spent nearly $10 billion on cybersecurity contracts in 2012. That number is projected to reach more than $14 billion by 2017. Industry professionals and government technology leaders expect cybersecurity to be the fastest growing area of federal IT investment during the next few years, according to a recent Deltek survey.

It shouldn't come as a surprise. In an August 2012 study from the Government Accountability Office, 18 of 24 major agencies reported inadequate information security controls, while inspectors general at 22 of those agencies identified information security as a critical management challenge.

Against this backdrop, a few must-know highlights can be valuable in securing agency networks.

CORBIS

PUBLIC-PRIVATE PARTNERS

A significant portion of the federal government isn't government per se—it's the contractors that provide the myriad goods and services that keep agencies running. So, it stands to reason that many cyber threats to govern-

ment involve private sector networks. For a cybersecurity policy to have teeth, it must reflect a meaningful level of cooperation between public and private institutions.

The Obama administration laid the groundwork for such cooperation with a much-anticipated Feb. 12 executive order authorizing new cybersecurity policies for critical infrastructure. Under the order, private operators of dams, electricity grids, financial institutions and other critical components can take part in an experimental program in which government agencies provide contractors with timely classified information on evolving threats.

But the order falls short of a full solution in at least one key way. While agencies would inform contractors about threats they've detected, private sector partners would not be required to close the loop by reporting on threats they have seen.

In addition, while a section of the document outlines steps agencies must take to protect personal information in these exchanges, privacy remains a concern among some members of Congress.

By and large, the order is only a starting point for shoring up cybersecurity. There is more to come, almost certainly in the form of legislation.

HACKTIVIST ATTACKS

"Hacking" often is defined as computer corruption for its own sake: Geeks showing off their prowess through random malice. "Hacktivism" is another phenomenon entirely. Groups like Anonymous, Telecomix and Team GhostShell typically have an agenda—a political or social point of view they express through the digital equivalent of breaking and entering.

The federal government is a high-profile target. In January 2012, Anonymous members angered by the death of an Internet activist facing federal charges, broke into Justice Department networks and threatened to release sensitive information.

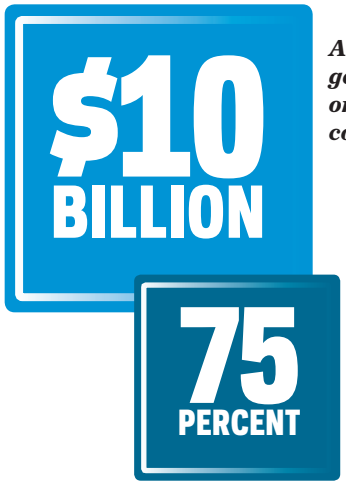
In December 2012, hacktivist group Team GhostShell claimed to have leaked 1.6 million account details belonging to federal institutions such as the Federal Bureau of Investigation, NASA, the Pentagon and Interpol.

For those who manage agency networks, hacktivism looms as a significant threat. With their inherently partisan agendas, hacktivists will continue to be attracted by the political nature of government operations.

NEXT-GEN FIREWALLS

It seems anything called a next generation firewall would be an unalloyed benefit. Digital firewalls fulfill a crucial function in defending networks from

FOR A CYBERSECURITY POLICY TO HAVE TEETH, IT MUST REFLECT A MEANINGFUL LEVEL OF COOPERATION BETWEEN PUBLIC AND PRIVATE INSTITUTIONS.



Amount the federal government spent on cybersecurity contracts in 2012

Portion of major agencies in a 2012 GAO survey that reported inadequate cybersecurity

intrusion. New and improved versions ought to be welcome, but the execution is a bit more complicated.

In brief, next-gen firewalls broaden existing protections and add capabilities in areas such as deep packet analysis, intrusion detection systems, securing application traffic and anti-malware. The technology gives administrators enhanced ability to control and manage their defenses.

But a few obstacles make adoption of next-gen firewalls less than a slam dunk.

One issue is the lack of common standards. Vendors come onto the court with a range of products that cannot be easily compared to one another due to a disparate variety of features and functions. Some products lack critical features or include unnecessary capabilities that degrade system performance.

Another challenge in launching new security technologies is preparing the employees involved. A new firewall can require certain skills or at least a different approach to operations. Network administrators must be trained and users need instruction on how to handle links, attachments and other potential hazards under a new structure.

NEW AND IMPROVED DIGITAL FIREWALLS OUGHT TO BE WELCOME, BUT THE EXECUTION IS A BIT MORE COMPLICATED.

INTERNAL TRACKING

Two basic truths for federal employees: Everything you do with a keyboard can be seen, and your agency is probably looking.

YouTube, Facebook, instant messaging and the allure of personal email, make it hard to keep a chair warm for eight hours a day and not dabble in some private Internet activity. Easily available software allows your boss to see all of this, and there's no clear constitutional guideline laying out the limitations.

Thanks to the disclosure of government information on the WikiLeaks website, agencies have become fixated on information flow, resorting to some extra-vigilant snooping. Last summer the Food and Drug Administration caught congressional heat for capturing employees' keystrokes after some 80,000 pages of information FDA collected ended up in the hands of contractor Quality Associates Inc. of Fulton, Md., which posted the information online.

Critics say FDA overreacted with such close tracking of employees' computer activity. But it's unlikely government agencies will abandon their oversight efforts. Federal employees should assume their communications are an open book. Privacy advocates may grouse, but the actions of workers in government or private sector typically are considered fair game for any employer looking to monitor internal activity.

CYBERSECURITY
NEED TO KNOW MEMO

ARE YOUR APPS SAFE?

Find out with a free security scan from F5.

Take advantage of F5's joint solution with Cenzic to find application vulnerabilities and patch them immediately. Schedule a free scan with Cenzic to see how you can reap the benefits.

- **Improve enterprise security** with Dynamic Application Security Testing.
- **Quickly mitigate risks** via integration with F5® BIG-IP® Application Security Manager™ (ASM).
- **Reduce your organization's risk** exposure with an easy, and cost-effective combined solution.
- **Protect your apps** from the OWASP Top Ten vulnerabilities while achieving compliance.

F5 and Cenzic

Cenzic provides application security to continuously assess cloud, mobile, and web vulnerabilities, helping organizations of all sizes protect their reputations. Cenzic solutions are used in all stages of the software development lifecycle, but most importantly in production, to protect against new threats for the life of the application.

Quick, flexible solution: Available as a cloud-based subscription with self- or managed-service options—with nothing to install.

Consolidated management: Tight API integration with F5 lets you assess and block vulnerabilities directly from the BIG-IP ASM GUI.

Immediate, accurate results: Cenzic security produces automated, near-instantaneous results with minimum false positives.

Clear, efficient reporting: Web-based dashboards and a prioritized vulnerabilities list with risk score provide easy insight into your security environment.

For more information about Cenzic, visit **cenzic.com**.

Visit **http://interact.f5.com/f5freescan** to assess your apps today.