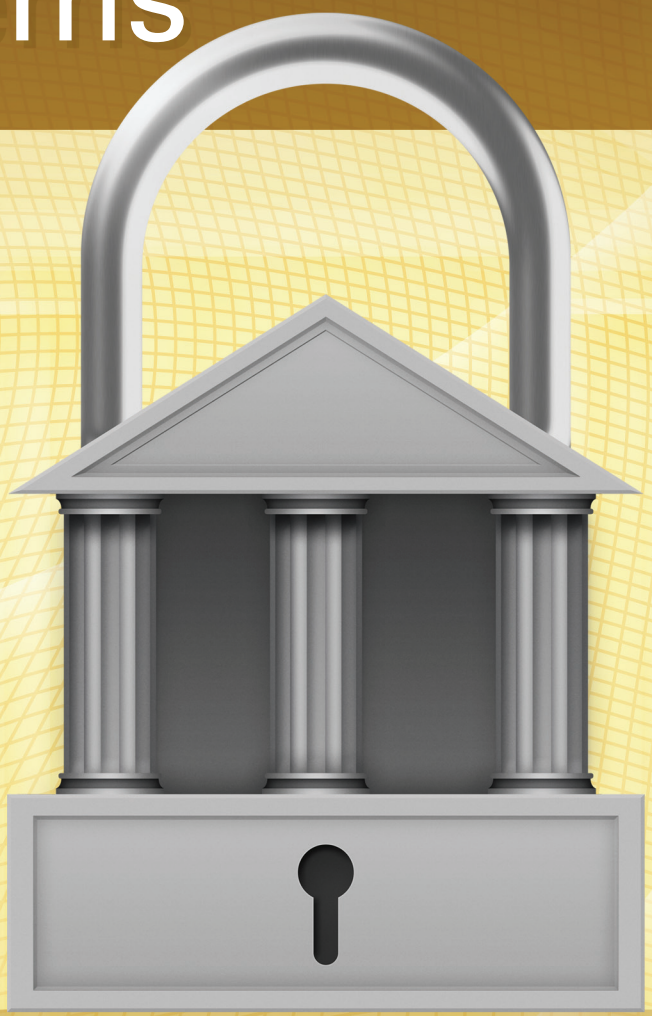
Feature articles & full report available for download at: www.FCW.com/SecuringGovSystems

Securing Government Systems



Inside

FISMA, compliance and the rise of the APT

Security professionals will tell you that compared with 10 years ago, government IT security practices are vastly improved. Back then, security was very much an ad hoc approach that varied greatly among agencies and for which erecting a firewall was considered state of the art, if security was considered at all.

Now, driven by regulations such as the 2002 Federal Information Systems Management Act (FISMA) and the Department of Defense Information Assurance Certification and Accreditation Process, IT systems security is a mandated focus for all agencies that have to adhere to a complex series of requirements.

It's become a very visible game of political football. Heaven help those executives whose agencies receive a D or, God forbid, an F on the House Oversight and Government Reform Committee's annual FISMA compliance score card that's compiled from data that agencies provide to the Office of Management and Budget.

Therein lies the main criticism that observers both inside and outside government have leveled at regulations such as FISMA: Agencies hustle to get as good a rating as they can each year, but even an A+ doesn't guarantee that IT systems are secure. If they're compliant when the audit is completed, they may no longer be so the next day. All FISMA compliance delivers is a one-time snapshot.

It's become a seductive alternate for real IT security, said Rob Lee, a director at information security consultant Mandiant and the curriculum lead for digital forensic training at the SANS Institute. He was also a founding member of the Air Force Information Warfare Squadron.

"Compliance is very measurable and security is not because it's very easy to say this is how well we're doing," he said. "As a result, agencies almost have to become compliance driven rather than actually security driven."

Compliance is the bed on which organizations fall when security fails, he said, "but it's a very minimal standard. We can do so much better than that. But even reaching that minimum standard is a very complex process for a lot of organizations."

OMB admitted in its recent fiscal 2010 report to Congress on the implementation of FISMA that this compliance mindset has been the controlling factor for FISMA over the years. FISMA has become just an additional compliance exercise that was related to but removed from the information security mission, it said.

However, OMB also said, as it became clear that compliance alone would never get the federal government to the right level of information security, many agencies have started to develop new ways to protect their systems that often go well beyond that required by policy or regulation.

Other parts of the government have begun to pick up on these developments to move FISMA implementation toward the real-time detection and mitigation of security vulnerabilities, OMB said.

However, government still has a long way to go to improve its security, even by those minimal standards set by FISMA compliance. As reported to OMB by the inspectors general of the 24 federal agencies that fall under the 1990 Chief Financial Officers Act, crucial areas such as systems configuration management, with just 25 percent of agencies compliant, and account and identity management at 21 percent, leave many government systems open to attack.

Changing long-held mindsets about security is the basic limitation, said Prem Iyer, director of the information security practice at Iron Bow Technologies, an IT solutions provider based in Chantilly, Va.

"When we talk to government customers, we find, unfortunately, that there tends to still be a very reactive approach to security," he said. "They tell us that they have to wait for an incident to happen, and then they'll get the budget to go and procure a solution to help address it."

Iron Bow tries to push those customers to take a holistic approach to security, to move from reactive to something

continued from page s2, FISMA, compliance...

more active and eventually to a fully optimized approach, Iyer said, as opposed to their current attitude, "which is very point solution oriented."

Meanwhile, the expanding universe of attackers is not waiting for government security to catch up to it. The number and kinds of attacks aimed at IT systems are increasing.

The number of incidents reported to the U.S. Computer Emergency Readiness Team totaled more than 107,000 in fiscal 2010. That was down slightly from the number for the previous year, but the number of federal-only incidents was up 39 percent compared with fiscal 2009, at nearly 42,000 incidents.

Introducing malicious code through multiple means, such as phishing, viruses and logic bombs, were the most widely used methods of attack. Those accounted for nearly a third of the total incidents reported by federal agencies in fiscal 2010.

Incidents Reported to US-CERT by Federal Agencies in FY 2010

Incidents Category	# Incidents	% Total Incidents
Unauthorized Access	5,775	13.8%
Denial of Service	23	0.1%
Malicious Code	12,864	30.8%
Improper Usage	7,329	17.5%
Scans, Probes and Attempted Access	4,419	10.6%
Under Investigation/Other	11,336	27.2%
Total	**41,776**	**100.0%**

Source: OMB Fiscal 2010 FISMA implementation report

However, even this doesn't adequately describe what many observers see as the biggest threat to government systems: the advanced persistent threat.

APTs are not that new. They have been seen in the wild for some years, and DOD in particular has been actively trying to develop defenses. But as some recent incidents showed — notably the Stuxnet worm that targeted various Iranian facilities in 2010 — these kinds of attacks have improved dramatically in terms of their sophistication and their ability to target individual systems and even pieces of data.

Stuxnet used a number of ways to get into the Iranian computers, such as zero-day vulnerabilities and default passwords, and then was able to stay hidden for days while it sought out and inflicted damage on Iranian supervisory control and data acquisition systems.

But Stuxnet was actually an anomaly as far as APTs are concerned. Because it was malware designed to operate in systems that were not connected to the Internet, it had to carry everything it needed to inflict damage in its own code. And it was that stand-alone status that made it vulnerable to detection.

APTs that attack systems that are connected to the Internet don't need to do that. After the malware has gained entrance into a system, which it could do with multiple attempts using a dozen or more separate methods, it could lie in wait for days, weeks or months, surveying systems for potential exploits. When it finds one, it could gain a connection to the outside by, say, getting a system user to click on a PDF and download its payload.

"The APT comes in there and suddenly they have system level privileges," Lee said. "Now [security people] say the APT must have X, Y or Z that can be detected but I say that, if they use an exploit no one has seen before, we'll never be able to detect it, and suddenly they're no longer persistent on the machine itself because they want to protect their zero-day weapon."

The government is facing attackers who are vastly more sophisticated and better funded than the lone individuals who were the main threat some years ago and who simply did it for the challenge of it and to flesh out their hacking skills or were opportunistically looking for data here and there.

That picture is now almost quaint. Hackers now are basically employees of organized crime or work for other nations, said Shon Harris, president of Logical Security, a computer security consulting firm and another former member of the Air Force Information Warfare Squadron.

Although it may guarantee that various security practices are in place, compliance with FISMA or other regulations is no match for them.

"We have a huge, false sense of security because we have our anti-malware, our personal and antivirus firewalls, and all these other defenses, but these only capture some 42 percent of the malware that come into the system," Harris said. "Government organizations can do every single thing right, and still be compromised and not know about it." ▲

Continuous monitoring: The new approach to compliance

If many of the problems with federal IT security come from the snapshot effect of adhering to yearly audit requirements of the Federal Information Security Management Act and other regulations, one answer might be to increase the frequency of those audits. Continuous monitoring of agency systems and security configurations is the new target for Congress and the Obama administration.

In March, Rep. James Langevin (D-R.I.) introduced the Executive Cyberspace Coordination Act, a House companion measure to the similar Cybersecurity and Internet Freedom Act introduced in the Senate in February. The measure would require agencies to undertake automated and continuous monitoring of their systems to ensure compliance and identify deficiencies in their IT security and risks to that security.

In its report on the fiscal 2010 implementation of FISMA, the Office of Management and Budget said agencies need to be able to monitor security-related information across the enterprise "in a manageable and actionable way," and a well-designed and well-managed continuous monitoring program "can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information."

In a December 2010 draft of its Special Publication 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," the National Institute of Standards and Technology described continuous, ongoing monitoring as a critical part of its overall risk management framework for information security.

A primary goal of continuous monitoring is, as much as is practicable, to apply automated remediation to security vulnerabilities that are found. That takes the need for human intervention out of the picture. Human intervention and the errors and delays that result from it are credited for many of the lapses in IT security.

Continuous monitoring is the right direction for agencies to take because, with the way things are going now with advanced persistent threats and other modern vulnerabilities, security is no longer about what you know — it's about what you don't know, Iron Bow's Prem Iyer said. And that's a complete switch from the mindset of the past 15 years of IT security, which has been organized around recognizing the signatures of known methods of attack.

"When we talk to customers it's about why they have all of these security solutions and processes in the first place," he said. "And then we point out that, if they are not being monitored in real time, the organization is probably not seeing the main thing that this security is catching, which is the zero-day threat."

Zero-day threats are malware that exploit unknown vulnerabilities in an organization's security, breaching defenses during the time the malware detects the vulnerability and when software developers create a patch for it. In the case of stealthy APTs, which are designed to be undetectable once inside a network or system, that first breach is all they need to be effective.

Along with using best practices, such as intrusion detection and malware protection technologies, continuous monitoring will need others such as security information and event management suites of event-logging tools and centralized security management dashboards that consolidate information provided by all of the automated scanning. Those tools would give network and security management personnel a near real-time view of the enterprise security status.

However, before that is possible, standards such as the

continued from page s4, Continuous monitoring...

Secure Content Automation Protocol (SCAP) have to be recognized and used throughout the security industry. SCAP is a suite of specifications that standardizes the way security software products recognize and name security vulnerabilities and configurations.

"SCAP is not one of those sexy security issues," said Shon Harris, president of Logical Security. "But until we can get a standardized way to call the same vulnerability and the same asset by the same name, we are never going to get our stuff together and we are never going to be able to do continuous monitoring."

Now, if a security professional were to do a certification and accreditation on a system, a checklist of different configurations of Web browsers, operating systems and so on must be completed, Harris said. That can take hours or even days, and further delays then happen because of paper work that has to be filed and an approval process that has to be navigated.

SCAP and other automation protocols ensure that this can happen continuously in a standardized way, and all the necessary reports are generated and communicated in a standard fashion, no matter what security products are being used.

Despite OMB's assertion in its FISMA report that, in fiscal 2010, the federal government "shifted from periodic security reviews to continuously monitoring and remediating IT security vulnerabilities," most agencies clearly have some way to go before they get there. According to the inspectors general at the 24 agencies covered by the Chief Financial Officers Act of 1990, nearly two-thirds of those agencies need improvement in continuous monitoring.

But that's something they likely won't be able to dodge, even if they wanted to, because several new federal reporting and implementation tools will require it.

Cyberscope, which was launched in fiscal 2010, is an interactive data collection tool that can capture the kinds of feeds produced through continuous monitoring and assess agency security postures. In April 2010, OMB directed that all agencies develop an approach for reporting their security compliance through Cyberscope, to include direct feeds from monitoring systems.

CyberStat, which will be introduced in fiscal 2011, is a management model that will enable the Homeland Security Department to quickly evolve new security metrics to gauge the effectiveness of agency security. Together, Cyberscope and CyberStat are expected to give the federal government a new level of information about risks to information systems. ▲

Is the future in secure systems or secure data?

If the future of threats against networks and systems is mostly of stealthy advanced persistent threat kind, is it safe to assume that some systems will be penetrated and attacked no matter what kind of security is put in place? If the main target of these attacks is information and data, why not focus on securing the data itself?

In some ways, that would be a return to the approach that ruled 15 years ago when firewalls were first deployed to protect the perimeter of the enterprise. The idea then was not to protect networks or systems but the data that traveled through and among them.

Even without APTs, the threat today from data leakage through everyday use by people who have no ill will at all should be enough to promote the idea of data security in organizations. And with the current use of portable storage devices such as USB devices and CDs, growth in mobile communications, and explosion in the use of things such as tablet computers and smart phones, there's no longer much of a perimeter to defend.

"We're at an interesting place right now where we finally get how to lock down the file servers and the database, and where we are doing a much better job of protecting the central repositories where the sensitive data resides," said Shon Harris, president of Logical Security, a computer security consulting firm. "If the data just stayed in the database, then life would be terrific. But people have to take a little piece of that data and put it into an e-mail or some other application to use it."

And after it's outside the database, data is no longer protected by the controls placed on the database itself.

The problem of data leakage led to the rise of data loss prevention (DLP) solutions, software that can monitor data in motion on the network, at rest in the data center, or in use at various points, such as workstations or mobile devices. The software automatically detects confidential data in any of those states and protects it by enforcing security policies to prevent it from ever leaving the enterprise.

For data that goes outside the enterprise, technology such as information rights management has emerged over the past few years as a necessary complement to DLP. It attaches controls to the particular pieces of data that may have been copied to a USB device, laptop or CD or e-mailed to someone outside of the enterprise, restricting who can read, alter, print or even forward that data.

That doesn't obviate the need for an enterprise defense-in-depth strategy and protection of what remains of an organization's IT perimeter, but that's not the be-all of security today.

"Absolutely there needs to be a movement to object centered security," said Prem Iyer, director of the information security practice at Iron Bow Technologies. "Even if I lose data from my own control, I still need to be in the position of implementing policies on that data and to ensure that it's not being viewed by anyone that doesn't have a need to know."

That's even more vital in the age of the APT. Most observers now believe that a good number of government computers have been penetrated by APT malware and that APTs have been resident in those systems for some time. On any given day, APTs are probably accessing and stealing sensitive government data without agencies being aware of it. ▲

The cautionary lessons of WikiLeaks

If any one recent event points to the need for things such as data loss prevention and information rights management, it's the release in 2010 of hundreds of thousands of sensitive Defense Department and State Department documents and diplomatic cables by WikiLeaks. Ironically, it wasn't caused by an advanced persistent threat or other sophisticated malware but by a well-known threat: a knowledgeable insider.

Still, it had the same effect. Shortly after the publication of the documents by WikiLeaks, OMB Director Jacob Lew ordered all federal agencies to review their procedures to prevent similar leaks and limit potential vulnerabilities, such as how documents could be downloaded and distributed.

"Such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure that users do not have broader access than is necessary to do their jobs effectively, as well as implementation of restrictions on usage of, and removable media capabilities from, classified government computer networks," he wrote in a memo.

DOD responded with a slew of new and updated security measures, including issuing 500,000 hardened smart cards to secure network users, implementing a host-based security system that centrally monitors system configurations, deploying a device control module that disables the use of removable media except in very limited cases, and considering the possible future use of an audit extraction module, developed by the National Security Agency, that can use existing audit capabilities on host-based security systems to report questionable behavior.

However, the DOD response also highlighted some of the problems with using security such as DLP or IRM. As DOD CIO Teresa Takai told Congress in March, using role-based software to limit users only to the information they are entitled to is feasible, but it depends on defining the many different roles that users can play — no easy task — and identifying the information they need to fulfill those roles.

It's the same problem that plagues the implementation of identity management systems. That technology has also been tagged as vital for government security. But in the context of what some government employees are asked to do, how do you define their identity?

At DOD, as Takai pointed out, intelligence analysts and operations planners need access to a wide range of data in order to do their job, and it's frequently of the most sensitive kind. In that instance — something that's similar at many agencies across the government — how do you apply DLP and IRM? ▲

Finding the right people

In the end, the biggest problem facing government when it comes to security in the age of advanced persistent threats and advanced malware is not the availability of good technology. There's already plenty of that. It's the dearth of the security professionals who know what to do with that technology and how to apply it to hunt for and deal with the threats.

Consider the situation the government faces. Go back five years or so, when most attacks against government systems were from lone hackers who attempted their exploits as part-timers. Many of them were smart enough but had limited resources.

The adversaries today — at least those that government needs to take the most notice of — are full-time employees of well-funded criminal or national organizations. The attacks are highly sophisticated and very targeted, and they are designed and controlled by people who can afford to be very patient. It's a whole new ballgame.

Countering APT malware requires an extremely high level of skill, said Stephen Northcutt, CEO of the SANS Institute.

"Incident responders of this type can understand malware they've never seen before, which is quite a skill," he said. "There's a rapidly growing need for these people, and right now, both government and the defense industrial base has been a little slower than banks, insurance companies and others with deep pockets in making the investment."

A senior professional at the top of his or her game can bring in $200,000 a year in many markets in the United States, he said, and even more than that in the really expensive markets.

Government actually spends more money on security than industry does, Northcutt said, but it doesn't spend it wisely. The average IT department in government, especially in the Defense Department, will have more people with information assurance or security in their titles than you will find in industry, "but because the pay rates are lower, so is their skill level," he said.

Because there are so many aspects to security management and technology, security professionals need a wide range of skills if they are to prosper in today's environment, said Shon Harris, president of Logical Security. They have to understand intrusion detection and intrusion prevention and how to run those systems, they have to understand firewalls and identity management, and they need to have basic network skills.

People think they have those things, she said, but many in the security field today don't have even that foundational base of knowledge. They don't necessarily understand how a computer works from the ground up, and they don't understand how the protocols and various software work.

"I've taught security for 12 years to every three-letter organization, to federal agencies, to all of the large banks, and I'm constantly blown away by the stuff so-called security professionals and engineers don't know," she said.

Even when agencies seem to be doing the right thing, it's simply not enough to counter today's threats. Many have formed incident response teams to fight intrusions, for example, but most of them are made up of people who normally have other duties to perform. They get pulled off those for three or four days to tackle the incident then pick up their regular jobs afterward.

That was fine in the past, when these teams would, once they had determined what the intrusion was, simply pull compromised systems off-line to reinstall them. And that might have been enough to prevent attacks from advancing, said Rob Lee, the lead for SANS' digital forensics training.

"But adversaries today are using techniques that basically put them on so many machines in the network it's like playing a game of Whac-a-Mole," he said. "You can rebuild a specific machine, but you'll find so many other systems and servers that have been compromised that you'll never be able to make any headway."

continued from page s8, Finding the...

The adversary's strategy is to be around for the long term and simply wear down incident response teams until they are too exhausted to continue, Lee said.

Agencies are starting to realize the need for dedicated response teams, he said, and there's progress evident in other areas. Two years ago, you would never have seen a dedicated malware analyst inside a government agency, he said, and now there are hundreds of them.

The problem is they are "not very good," he said. And training people from scratch will not meet the immediate need, as it takes at least a couple of years to get someone up to the level of skill that's needed to deal with modern malware.

The individuals who can do this task well are in very high demand; there just aren't enough of them, Lee said. Until acquiring the skills needed to deal with the kind of malware APTs use becomes a prerequisite for government security professionals, those threats will continue to be a problem. ▲

ARE YOU CONFIDANT YOUR ENTERPRISE IS SECURE?

INFORMATION SECURITY RISKS AND THREATS MAY BE GOING UNCHECKED.

Everyday your IT environment is vulnerable. New cybersecurity threats are multiplying and evolving at an unprecedented rate. It's difficult to know for sure that your assets are safe and secure.

Make sure your Information Security is:

- Proactive
- Real-time
- Optimized
- Mission-enabling

CONTACT THE IRON BOW SECURITY TEAM TO ASSESS YOUR CURRENT IT ENVIRONMENT

GO TO **WWW.IRONBOW.COM/SOL_SECURITY.HTM**

McAfee nitrosecurity

IRON BOW TECHNOLOGIES