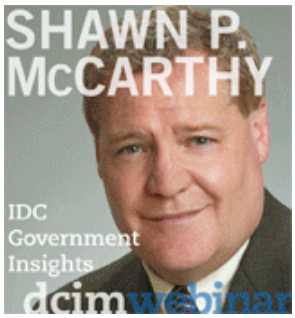

Infrastructure Optimization»

Policies, Not Tools, Drive Cloud Security

With plenty of cloud security tools available, federal IT managers focus on procedures and processes.

Karen D. Schwartz

posted March 12, 2012 | Appears in the Focus on Cloud Computing issue of the *FedTech Magazine* e-newsletter.

Related Articles
Review: Symantec Endpoint Protection.cloud
Serving Up Anytime, Anywhere Apps Over a Private Cloud
The Dynamics of Cloud Security
FedRAMP: Ready, Set, Launch for Cybersecurity
Six Tips to Keep Video Conferencing Sessions Safe
Editors Picks

DIA's Michael Mestrovich: IT Innovator-in-Chief
Saving Green by Going Green
Network Security: More Than a Technology Challenge
The Changing Role of the CIO

The Nuclear Regulatory Commission depends on Patrick Howard's advice when it comes to security in the cloud.

As the agency's chief information security officer, Howard says there are plenty of tools that offer continuous monitoring and visibility for public-cloud applications while maintaining 24x7 security.

"The tools aren't the issue," Howard says, adding that the real challenge is having the procedures and processes in place to help decide if an application should or should not be placed in the public cloud.

Howard says any highly sensitive information is off limits for a public-cloud application. However, the NRC is fine with low-priority data moving to the cloud with controls based on the Federal Risk and Authorization Management Program. FedRAMP offers a standard approach to security assessment, authorization and continuous monitoring for cloud products and services.

Rod Turk, chief information security officer at the Patent and Trademark Office, largely agrees with Howard's approach. Turk says his organization has focused mainly on private-cloud implementations, mostly to have more control over the data and the process. But over time, more cloud deployments are inevitable, especially applications at least partially in the public cloud.

For all types of cloud implementations, Turk insists that security is as much about processes and due diligence as it is about tools. For anything the agency considers for the cloud, a team conducts a business case and full analysis to determine whether it makes sense to proceed.

"Once we decide to move forward with a cloud implementation, we make sure to use a provider and processes that we trust will reduce our risks," he explains. "We make sure we research where it will reside, how it will be hosted, and that we have reduced the risk to the point where we find it acceptable."

33%
The percentage of IT security executives polled who think cloud infrastructure environments are as secure as on-premises data centers

SOURCE: Ponemon Institute, October 2011

Both Howard's and Turk's views about what it takes to remain secure in the cloud are common among federal government security professionals, at least partially because of the strict security guidelines set by FedRAMP.

Yet for any organization with software, infrastructure or platforms in the cloud, it's critical to identify threats and vulnerabilities in real time so they can be acted on and resolved quickly, says Renell Dixon, a managing director in the federal practice at PricewaterhouseCoopers, a global consultancy firm.

"When you're talking about the cloud, the window of opportunity between the time a threat is located and the time you are fully protected is very small," she says. "It's important to put something in place that manages that process in real time by continuously monitoring and fixing problems as they occur."

Cloud Security: Help Is on the Way

Security is the biggest reason organizations hold back from moving to public-cloud services. In response, several of the most prominent security manufacturers have released products to ease these concerns.

One category is cloud-based e-mail security. Products such as *Symantec.cloud* and Panda Cloud Email Protection offer virus and spam protection, along with content and image control. Symantec also offers a product that delivers instant messaging protection in the cloud.

Cloud-based security for the web is another major category, with offerings that include *Trend Micro's* SecureCloud, *McAfee* Cloud Security, *Panda Cloud Office Protection* and *M86* Secure Web Service Hybrid. These services block malware and spyware and offer policy control and user authentication.

Providers also offer cloud-based security services that deliver continuous-monitoring trend analysis.

“It’s about identifying threats and vulnerabilities and acting on them quickly to prevent problems people are concerned about, like identity theft, denial of service and data loss,” explains Renell Dixon of PricewaterhouseCoopers.

Making the process quick and easy makes it more likely that mobile users will do it.

Disaster Relief

Understanding an agency's needs and testing to make sure they're met are keys to...

more »

Networking

Network Upgrades Meet the Need for Speed

As critical missions become more challenging, federal networks must find ways to remain...

Six Tips to Keep Video Conferencing Sessions Safe

When users connect from outside a private network, follow this advice to shore up...

more »

Mobile & Wireless

The Next Step in Telework

Despite some hiccups, most agencies are moving forward on telework adoption and growth.

5 Pointers for Backing Up Mobile Devices

Making the process quick and easy makes it more likely that mobile users will do it.

more »

Hardware & Software

Review: InFocus IN3914

This short-throw projector is a great alternative to an interactive whiteboard.

Reclaim the Copy Room with Managed Print Services

Print management can save money and boost productivity.

more »

Infrastructure Optimization

Security

Storage

Networking

Mobile & Wireless

Hardware & Software

Management