STATETECH Technology Insights for Leaders in State & Local Government

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Infrastructure Optimization

Security

Storage

Networking

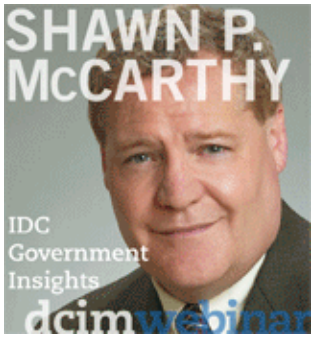
Mobile

Hardware & Software

Management

CURRENT ISSUE

Subscribe



Infrastructure Optimization »

Governments Take Different Paths to Cloud Security

IT managers at government agencies take different approaches to cloud security.

Karen D. Schwartz

posted March 13, 2012 | Appears in the Focus on Cloud Computing issue of the *StateTech Magazine* e-newsletter.

Related Articles
Serving Up Anytime, Anywhere Apps Over a Private Cloud
Review: Symantec Endpoint Protection.cloud
Review: Fortinet FortiGate–300C
Secure Storage
Achieving PCI DSS Compliance
Editors Picks

Governments Collaborate Across Borders
5 Tips for Optimizing Load Balancers
M2M Networks Make Inroads
Surveillance Cameras Serve Lookout
State by State
In this article: Montana | New York

Carl Purdy is used to making special trips to handle a variety of IT issues. Although he may have to venture out from time to time, the IT Manager of Jefferson County, Montana, says he no longer has to drive across the county to manage security servers.

About two years ago, Purdy moved security management from physical servers running Panda's antimalware product to the cloud. Today, he relies on *Panda Cloud Office Protection*, a cloud security service that lets him connect via the web and renew virus definitions. That's much easier than the previous system, which required Purdy to travel throughout the county to manage the security on servers, desktops and notebooks.

"I can sit at my dining room table, which is 30 miles from my office, and take care of whatever needs to be taken care of," Purdy says. "If a user gets a new notebook, I just send them an e-mail with instructions to click on a link. When they do, it automatically installs the antimalware products on the notebook with all of our credentials set. I never need to have their notebook in my hands."

"Security is always up to date and installed with the protection I want, with the ports open and closed that I want open and closed," he says. "It's much easier to manage."

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 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."

A Familiar Tune

Dan Srebnick, New York City's chief information security officer, looks at cloud security a bit differently. He says security issues in the cloud can be handled much the way they are in the data center.

"My philosophy is that a data center is a data center, so aside from the methods you use to run and provision it, we set out to see if we could apply some of the tools we use internally to the cloud," Srebnick says.

Srebnick uses the same security tools he runs in the data center — the *McAfee Vulnerability Manager* host vulnerability scanning system and *IBM Rational AppScan* for application vulnerability scanning. He also set up a special instance of the McAfee tool outside the firewall to manage cloud traffic.

So far, the system is working well. Earlier this year, the department set up a public cloud using *Microsoft* Azure

to let people register for a limited number of tickets to a parade for the New York Giants after they won the Super Bowl. The site was deployed very quickly to handle a large anticipated load. Using the same security tools deployed internally, the IT team could identify and remove security vulnerabilities.

"When it comes to the cloud, it's important not to forget that it's the basics of IT security that are the 'gotchas,'" Srebnick says. "If you fail to do the basics within your own environment or within the cloud environment, the bite marks are the same."

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

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.

About the Author
Karen D. Schwartz
Karen Schwartz is a freelance technology writer based in the Washington D.C. area.

Trackback URL http://disqus.com/forur

Infrastructure Optimization

License Management for the Virtual Data Center

Follow these tips to achieve software licensing compliance.

How DCIM Tools Can Improve Data Center Management

Analysts expect fast adoption in the next few years.

…more

Security

Achieving PCI DSS Compliance

Take these steps to better protect citizen cardholder data.

Review: Fortinet FortiGate–300C

The all-in-one FortiGate–300C security appliance ably protects networks from the web's…

…more

Storage

5 Backup Pointers for Mobile Devices

It's up to the IT team to make this must-do job as simple and speedy as possible.

Get the Most from Deduplication

Follow these tips for achieving maximum efficiency from your storage system.

…more

Networking

Make the Move to Managed Switches

Organizations opt for managed switches to enjoy reliability, redundancy and future-…

Private Eyes

Learn how to keep video conferencing sessions safe from interlopers.

…more

Mobile

Counties Forge BYOD Policies

Initiatives address the security and management issues associated with employee use of…

Gain Visibility into Mobile Devices

Here's one product to manage the fleet, plus facts and figures about mobile…

…more

Hardware & Software

Electronic Patient Care Record Systems Aid Emergency Response

ePCR improves data accuracy and billing efficiency.

Symantec Altiris Asset Management Suite 7.1

Suite keeps a close eye on IT hardware and software.

…more

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management