EDTECH ™ FOCUS ON HIGHER EDUCATION

Brought to you by:

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management

CURRENT ISSUE

Subscribe

SIGN UP FOR

EdTECH

E-NEWSLETTERS

Follow EdTech

RSS Feed

Connect With CDW

LinkedIn YouTube Spiceworks

Like 5k

EdTech

HIGHER ED SCOPE

Find out what your peers are doing around the country.

Home » Security

‹ previous   **next ›**

Authentication

Colleges Focus on Cloud Security

Campus IT shops make securing public-cloud apps a priority.

Karen D. Schwartz

posted March 14, 2012 | Appears in the Focus on Cloud Computing issue of the *EdTech Magazine* e-newsletter.

Like   Share   Spice

Related Articles

Serving Up Anytime, Anywhere Apps Over a Private Cloud

Review: Symantec Endpoint Protection.cloud

5 Tips for Securing Windows Desktops

Keep Those Notebooks Safe with Encryption

Up Close and Personal

Editors Picks

Three Easy Steps to BYOD

5 Tips for Optimizing Load Balancers

Why Computer Labs Are Still Essential On Campus

ADVERTISEMENT

Many colleges are taking their time signing on with public-cloud services. As a general rule, universities tend to adapt slowly to changing technologies, and the security of any cloud service is a big concern.

That's why Northeastern Illinois University in Chicago started with security. One of the university's first steps into the cloud was to migrate away from on-premises virus and spam filtering to cloud-based e-mail security. The university recently discontinued its use of _Symantec's_ on-premises _Brightmail_ system in favor of _Symantec.cloud_, a public cloud e-mail security service.

"We are always hesitant when it comes to the cloud, but we felt comfortable moving our e-mail security to the cloud with Symantec because security is what they do," says Kim Tracy, executive director of University Technology Services at Northeastern Illinois.

Symantec's expertise in security has already come in handy. The university has experienced a series of targeted phishing attacks, and the software provider, through its cloud service, has been helpful in reducing the attacks.

"I'm thankful we have Symantec to work on it," Tracy says. "They have a much better chance of fixing this problem than we could internally. We would just end up filtering out too much, including a lot of legitimate e-mail."

The move to Symantec's cloud service offers solid security and also gives Tracy's department the flexibility to easily add or delete users as their needs change. That's important, because the next step will be moving students to Gmail while keeping faculty and staff on the Symantec e-mail security system.

For any organization with software, infrastructure or platforms in the public 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."

Why So Cautious?

James Leoni, deputy CIO for University of Maryland's campus in Baltimore, is as cautious as Tracy when it comes to moving to the cloud. His campus is home to seven professional and graduate schools, including medicine and law. That means there's a lot of personal legal and healthcare information that must be protected.

Faculty and staff are advised not to use the public cloud for certain grants and collaborative documents in order to protect sensitive data. However, during the past year, the staff started allowing students to use Google Apps for Education and Gmail.

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

Recognizing they need to secure both internal applications and external public-cloud services, campus IT staff set up a system in which all incoming and outgoing e-mail or documents pass through a _Cisco Systems IronPort_ security appliance. The IronPort gear encrypts sensitive information using rules that match the unique policies of

the professional schools.

"So whether its e-mail in the public cloud or internal applications, it all goes through the IronPort appliance," Leoni says. "The beauty of this is that we were able to deliver security for our public-cloud applications by using our existing infrastructure."

Over time, Leoni expects more functions and applications to move to the cloud. One possibility, he says, is *Microsoft Office 365*, which provides cloud-based versions of its desktop, communications and collaboration software.

"The reality is that some of these cloud services are more secure than some of the servers people are running locally," he says. "We have one or two people running our student e-mail system, for example, but at Google, they have an entire security team. Hundreds of system administrators can offer more resources than one or two."

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.

Higher Ed Scope
For more stories on colleges in Illinois | Maryland
About the Author
Karen D. Schwartz
Karen D. Schwartz is a freelance technology writer based in the Washington, D.C., area.

Like

Add New Comment   Login

Showing 0 comments   Sort by newest first ⇕

✉ Subscribe by email 📶 RSS

Trackback URL http://disqus.com/forur

Classroom

E-Textbooks Versus Print Books: Will the Traditional Book Survive?

New CourseSmart study says college students are embracing digital textbooks.

Colleges Need to Upgrade Their Networks to Support Virtual Learning

A strong online learning program requires a robust IT infrastructure.

…more

Infrastructure Optimization

Which Apps Should Stay and Which Apps Should Go?

Try these guidelines when considering which applications to include in your organization'…

Cleaning Up Cable Management

Control data center cabling with these five steps.

…more

Security

Security Considerations for Virtual Learning

IT departments recognize they need a multilevel approach to security.

Windows AppLocker's Lockdown Limitations

Learn the cans and can'ts of this Windows authorization and prevention program.

…more

Storage

The Value of Storage Virtualization

Nondisruptive data migration, improved utilization and fewer points of management are…

NAS: Big Storage in a Small Space

Network-attached storage devices can fulfill the needs of both large and small…

…more

Networking

Colleges Need to Upgrade Their Networks to Support Virtual Learning

A strong online learning program requires a robust IT infrastructure.

Should You Disable IPv6 on a Windows 7 PC?

Several features depend on IPv6 to function properly, so proceed with caution.

…more

Mobile

4 IT Security Tips for BYOD

Everyone wants to bring personal devices into the classroom; these tips will help keep…

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.

…more

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management