COMPUTERWORLD

The challenges of cloud security

Beth Schultz
12.07.2010 kl 04:28 | Network World (US)

Some IT execs dismiss public cloud services as being too insecure to trust with critical or sensitive application workloads and data. But not Doug Menefee, CIO of Schumacher Group, an emergency management firm in Lafayette, La.

"Of course there's risk associated with using cloud services – there's risk associated with everything you do, whether you're walking down the street or deploying an e-mail solution out there. You have to weigh business benefits against those risks," he says.

FAQ: Cloud computing demystified

Menefee practices what he preaches. Today 85% of Schumacher Group's business processes live inside the public cloud, he says.

The company uses cloud services from providers such as Eloqua, for e-mail marketing; Google Apps for e-mail and calendaring; Salesforce.com, for CRM software; Skillsoft, for learning management systems; and Workday, for human resources management software. "The list continues to go on for us," he says.

Yet Menefee says he doesn't consider himself a cloud advocate. Rather, he says he's simply open to the idea of cloud services and willing to do the cost-benefit and risk analysis.

To be sure, the heavy reliance on cloud services hasn't come without a security rethink, Menefee says. For one, the company needed to revamp its identity management processes. "We needed to think about how to navigate identity management and security between one application and another living out in the cloud," he says.

Identity as a start

Indeed, rethinking identity management often is the starting point for enterprises assessing cloud security, says Charles Kolodgy, research vice president of security products at IDC. They've got to consider authentication, administrative controls, where the data resides and who might have access to it, for example.

"These are similar to what enterprises do now, of course, but the difference that it no longer owns the infrastructure and doesn't have complete access to the backend so it needs strong assurances," he adds.

Start-ups ServiceMesh and Symplified have addressed the need for strong cloud security assurances with offerings aimed at unifying access management. ServiceMesh offers the Agility Access, for use with its Agility Platform, which comprises cloud management, governance and security tools and modules, as well as the services managed under the platform.

Symplified offers Trust Cloud. Built on the Amazon Elastic Compute Cloud (EC2), Trust Cloud is a unified access management and federation platform that integrates and secures software and infrastructure cloud services, EC2 and Web 2.0 applications.

In its case, Schumacher Group uses the Trust Cloud predecessor, Symplified's SinglePoint, an identity, access management and federation service that gives users single sign-on access to multiple cloud applications. In addition, SinglePoint lets IT rapidly provision and de-provision access to all applications in one pass. It's looking into moving from the appliance approach to Trust Cloud, but isn't committed to the idea yet, Menefee says.

Helping hand, and then some

Beyond technology, the cloud services model gives rise to a new way of thinking about Schumacher Group's operational resources, Menefee adds.

"Large cloud providers have teams and departments tasked full time, 24/7, to do nothing but protect their customers' sensitive information and to find continuous improvements to their security, monitoring, intrusion control and so on. As a midsized organization, I don't have a full-time, multiperson department focused entirely on security. With cloud service providers I feel more secure because I get the same benefit as what a Fortune 500 or 100 company would get with a multitenant, secure environment," he says. And, should a security breach occur, "Those teams will be more equipped to do a rapid response than my internal people would."

Certainly with your enterprise data at stake, pushing cloud providers to deliver the security you need – and then some -- is perfectly reasonable. As Forrester analyst Chenxi Wang says, "Don't ever compromise any security goals or requirements just because you're moving to the cloud."

Cloud services providers should go the extra mile on security provisioning – and enterprises have to hold them to it contractually, Wang says. "If a cloud services provider says what you want isn't achievable or that it can't provide evidence, you say, 'Look, we'll go to another cloud provider or not to the cloud at all,'" she adds.

Schwan Food, in Marshall, Minn., used that tactic when planning a virtual disaster recovery architecture, says Cory Miller, senior IT operations manager for the multibillion dollar frozen food company.

"We told our providers, 'You are going to use our tools and we are going to extend them into your environment," he says. "And I'll do more of that as I expand more into the cloud."

The choice is simple, really. Force providers to work with what you have or find yourself working with yet another set of security tools and interfaces. Chances are, you can even get your security tool vendor to contract with the provider, Miller says.

Along those lines, Reflex Systems, whose virtual firewall Schwan uses to secure its virtualized infrastructure, works with Computer Sciences Corp. and Savvis. The goal is "bringing some consistency to security and management when moving between private clouds and public clouds," the company says.

Schwan fielded solicitations from a number of cloud providers interested in working with it as it examined how to extend outward, Miller says. However, when it came right down to it, not all cloud providers were receptive to Schwan's mandates. The technology match-ups were problematic for them.

"With several we turned around and said, 'We'll do this and if you're not interested in providing that capability or service to us, we'll go somewhere else and find someone who is," Miller says. However, he cautions, "we're considered very mature in our environment ... and I'm not sure smaller companies would have that luxury."

COMPUTERWORLD

But even small companies would be wise to look out to the future. If you're building a private cloud today with the thought of extending to the public cloud, then knowing what security tools your potential provider will or won't support could impact the technology choices you make, Miller adds.

"You don't want to have designed your private cloud and then find out that the external cloud has such different change management or encryption processes, for example, that it almost offsets the advantages you have in expanding or moving out into the cloud," he says.

Getting tough on cloud providers

As cloud services mature, vendors are working on tools and services to help -- if not outright encourage – enterprises to make these sorts of tough demands.

One such tool is Adaptivity's Blueprint4IT. With this IT design software, an enterprise would be able to create an IT security blueprint that takes into account factors such as access policies and the sensitivity of data while in transit and at rest, as well as the hardware and software components needed to keep data flowing securely from the internal network into the cloud.

"Take your requirements, generate a blueprint, and hand it to your service providers and say, 'Here's exactly how we'll be setting up our infrastructure and how you're going to guarantee it on the other side as part of our contract," says Tony Bishop, founder and CEO of Adaptivity. "Just like you'd hand a blueprint to a general contractor and say, "Here it is. Go build my house."

Or, he adds, enterprises could use Blueprint4IT to assess their service providers and help them score the maturity of their security architectures.

This desire of enterprise customers to conduct their own assessments of a provider's security architecture is something new, agrees Neil Ashizawa, senior manager of HP SaaS products and cloud solutions. Such requests aren't widespread right now, he adds, but HP does field them from time to time for its SaaS offering and expects to see the numbers grow as cloud services use matures.

Toward that end, HP offers Cloud Assure, which allows enterprises to scan and do automated penetration testing of networks, operating systems, middleware layers and Web applications for vulnerabilities. This allows the enterprise to get assurance that the cloud provider of choice will be able to carry application workloads securely and keep them safe from unauthorized access, Ashizawa says.

Where there's a will ...

As enterprises approach the public cloud, what they have to remember is that "not every application is going to make sense to be done securely in the cloud, but neither is it that the cloud can't be made secure enough for anything," says John Pescatore, a vice president at Gartner.

Even financial firms, government agencies or other companies with highly-sensitive data such as payment card information or medical records can find the necessary protections in the cloud if they look hard enough, Pescatore says. "I may say, 'That type of data can never go in the cloud or I might say, 'How about if I find a way to encrypt the data and store it in the cloud?'"

As an example, he cites a demonstration conducted late last year in which the Navy successfully showed it could use a commercial cloud infrastructure-as-a-service platform – in this case Amazon's EC2 – to

support its requirements securely. The demonstration included the use of Unisys' ultra-secure access control and security technology, called Stealth.

Developed for U.S. Department of Defense (DoD) war fighters, the Stealth technology provides data protection for Unisys Secure Cloud services. "The name sounds kind of cheesy at first but it's appropriate because it cloaks data just like what happens with Stealth planes and now boats," says Jason Noel, vice president of the Unisys global customer advisory practice.

When a cloud user logs in and authenticates to the access control mechanism, Stealth figures out who the user is and to which community of interest he belongs and with what security levels. From there, the user only has physical access to participating systems with those security levels. Before a packet traverses the server or storage network, Stealth uses a patented technology to break it into bits, which are then shuffled into three or four "piles." Stealth encrypts each pile separately and then sends them over an encrypted link. The process is reversed at the other end of the connection, Noel describes.

Another approach, Pescatore says, is to use dummy data in place of sensitive information out in the cloud. "Applications work fine but sensitive data like payment card information or personally identifiable information stays local," he describes.

Start-up PerspecSys offers this type of functionality, initially for use with the Salesforce.com CRM cloud.

The PerspecSys technology installs as a proxy server through which traffic to and from the salesforce.com domain gets routed. PerspecSys intercepts data from sensitive fields and keeps it local while sending randomly generated replacement values that protect the data while preserving the functionality available within the CRM application, explains Terry Woloszyn, company founder and CTO.

"We pre- and post process the requests and the results to make them look to the cloud user like it's all in salesforce.com," he adds.

This is an alternative to encryption, which is difficult to do with applications, like Salesforce.com CRM, that have prescriptive field lengths or which require searching functionality, Woloszyn says.

Clearly enterprises have much to think about as they consider using public cloud services. They've got to take a risk-based approach, as has Schumacher Group, with a strong focus on the data and what controls are needed.

Read more about data center in Network World's Data Center section.