Herding Cats:
Seeing Through the Fog

October 2010

BrandenWilliams
SECURE BUSINESS GROWTH

If you want an example of where I messed up, here's one. Instead of putting together content to fill 3,500 words of space, I waited until the last minute and will cram some cloud security thoughts into 750 or less. On one, on one! Set?

HUTT![1]

Aside from all the definitions that engineers have to come up with to justify "CLOUD FRIENDLY!" on a product slick, we will use the following assumption for the remainder of the article. Cloud services are dynamic, scalable, utility-based computing models that allow companies to take advantage of hardware, software, and platforms on demand without investing in building the entire infrastructure[2].

Cloud services come in two flavors--public and private. Both share common architecture on the back end, but private cloud models add more security, or just don't have public access. Cloud providers offer varying degrees of both models, but the key you need to remember is, "What keeps this data secure?" If the answer is a short "Not much," you might be in a public cloud. No worries, there are good uses for those services as well.

Let me walk through an example of where a public cloud model can help a business. Pretend you are a big e-commerce retailer and it's Thanksgiving. Are you ready to survive Cyber Monday as millions of us make use of our lunch breaks to shop for holiday gifts? If so, I bet that you have a ton of infrastructure that sits idle for the other 364 days of the year. Infrastructure that takes physical space, cooling costs, IT maintenance (salaries), and power to sit idle. Browsing a product catalogue is important to ultimately make a sale, but passive clicking consumes all of the above resources and does not drive value to the business.

What drives value is when I put my card number into the system to purchase something. That's also where we run into issues with public cloud infrastructures as that data needs to remain private. So what should we do?

What if you put your catalog into a public cloud that would scale to respond to demand, and when it came time to pay, you redirected the user to a private cloud, virtual, or bare metal server that you administered in your data center? The only costs you would be carrying would be those that support the money, not the shopping. Your catalog and pricing is probably not sensitive information. If you think your competitors don't know your offers and pricing, you are fooling yourself. So why not throw that into an infrastructure that can get you closer to utility-computing and pay for exactly what you use?

Private cloud providers have a bit of work to do over their public counterparts because the data they house is more sensitive. For example, using a Desktop as a Service (DaaS) provider that allowed your employees to connect virtually to an infrastructure that had all of your business applications must contractually provide assurances back to your company to ensure that the applications are available, maintained securely, and the data is protected.

Ultimately, when looking at cloud providers and what services to put into a cloud or virtualized infrastructure, you must consider the data itself. What kind of data are you pushing to the cloud? Where does it go (physically)? Do privacy laws and cross-border

FOOTNOTES

[1] *Why yes, I AM ready for some football!*

[2] *Check this post for one of the dangers that SMBs face with this approach: http://bit.ly/c81ey4*

problems stand to complicate your journey to the cloud? Does the added data security cost required to demonstrate compliance with initiatives like PCI DSS or HIPAA outpace the financial benefits of cloud services? Those are critical questions that any company toying with cloud services must answer.

Once you have a strategy, you must ask hard questions of your providers. Questions like: How do you secure my data? How do you keep my data separate from other customers? How do you prevent one customer's application mistake from taking down my services? How do you prove all of these claims? On what regular cadence will you validate these controls and send me the evidence? Do you indemnify me if you make a mistake?

It's clear that the journey to the cloud is certainly going to happen—the cost savings are too compelling to ignore. It's up to us to figure out how to do it securely.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH