Multi-Tenant Security Is More About the Neighbors Than the Model

Lori MacVittie, 2010-09-06

Scott Sanchez recently rebutted the argument that “Cloud Isn’t Secure Because It Is Multi-Tenant” by pointing out that “internal data centers are multi-tenant today, and you aren’t managing them as well as a public cloud is managed.”

Despite the truth of that statement, his argument doesn’t take into consideration that multi-tenant cloud security isn’t just about the risks of the model, it’s about the ***neighbors.*** After all, there’s no such thing as a “renters association” that has the right to screen candidate tenants before they move in and start drinking beer on their shared, digital lawn in a **public** environment. When an organization implements a multi-tenant model in their data center the tenants are applications with the same owner. In a public cloud the tenants are still applications, but those applications are owned by any number of different organizations and, in some cases, individuals.

IT’S STILL ABOUT CONTROL

With the exception of co-location and dedicated hosting, this is essentially the same risk that caused organizations not to embrace the less expensive option to outsource web-application and its infrastructure. Once the bits leave the building there is a loss of control, of visibility, and of ability to make decisions regarding what will and more importantly what ***won’t*** run on the same machine as a critical business application. If the bits stay in the building as Scott points out there’s still very little control afforded to the business stakeholder but there’s also less need for such concerns because every application running in the internal data center is ultimately serving the ***same*** business.

> Unlike the public clouds, the resources of the private cloud are shared only within the corporate community. They're controlled by the corporation, not a third-party vendor that has the ability to lease them to anyone it chooses.
>
> **Private cloud computing Takes Off in Companies Not Keen on Sharing**
>
> See full article from DailyFinance: http://srph.it/98APyl

And if somehow one of the applications in the data center, whether multi-tenant or not – manages to chew up resources or utilize so much bandwidth other applications starve, IT can do something about it. Immediately. When everything is running in the same controlled environment the organization has, well, more control over what's going on.

The public cloud multi-tenant model is different because the organization's neighbors may not be Mr. Rogers and they might just be Atilla the Hun. And even if they are harmless today there's no guarantee they will be tomorrow – or in the next hour. There's no way to know whether applications of the serious business kind or of the serious making-money-phishing kind are running on or near the organization's application. And that's important because there is very little (if any) visibility into the cloud **infrastructure,** which is also inherently multi-tenant and **shared.** There's no transparency, nothing that's offered to assuage the fears of the organization. No guarantees of bandwidth even if the app next door start spraying UDP packets like water from a fire-hose and saturates the ***physical network*** or any one of several intermediate network devices between the server and the boundary of the cloud provider's network. In many cases, the customer can't even be assured that its data (you know, the lifeblood of the organization) is actually isolated on the network from cloud boundary to application. They can't be certain that their data won't be silently captured or viewed by someone lucky enough to have rented out the room above their store for the night. Deploying an application that handles highly sensitive data in a public cloud computing environment is very nearly a crap shoot in terms of what kind of neighbors you'll have at any given point in the day.

THEN THERE'S BUSINESS RISK

Even if you can assure these reluctant organizations that it is completely secure, there's still *business* risk to contend with.

> Turning to business risk, the issues are more related to operational control and certainty of policy adherence. Some companies would be very reluctant to have their ongoing operations out of their direct control, so they may insist on running their applications on their own servers located within their own data center (this issue is not cloud-specific—it is often raised regarding SaaS as well as more general cloud computing services).
>
> The Case Against Cloud Computing, Part Two, CIO.com
> Bernard Golden

Much of that business risk comes not from the technology model of multi-tenancy, but from the *business model* employed by cloud, i.e. open-door, no-questions-asked, rent by the hour compute resources, as well as the policies that seem to prevent the level of transparency into the underlying infrastructure that might convince a few more organizations that the risks are offset by the advantages.

Some organizations will remain steadfast in their refusal to leverage public cloud. It may take until cloud as an implementation reaches full maturity and provides the control they require before they will consider public cloud an option, if they ever do. They'll certainly not be swayed by arguments that simply dismiss their concerns based on the assumption that their own security practices are flawed anyway.

Related blogs & articles:

- Why private clouds are surging: It's the control, stupid!
- Private Cloud Model Will Win over Public Cloud Model
- Cloud Today is Just Capacity On-Demand
- Cloud Isn't Secure Because It's Multi-Tenant
- Why IT Needs to Take Control of Public Cloud Computing
- Architectural Multi-tenancy
- F5 Friday: Never Outsource Control
- The Other Hybrid Cloud Architecture
- The Corollary to Hoff's Law
- Optimize Prime: The Self-Optimizing Application Delivery Network

- Optimize Prime: The Self-Optimizing Application Delivery Network
- Cool Hand Cloud
- The Three Reasons Hybrid Clouds Will Dominate

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com