THE ELEPHANT IN THE ROOM

CLOUD SECURITY AND WHAT VENDORS AND CUSTOMERS NEED TO DO TO STAY SECURE

Through this year-long series of whitepapers and webinars, independent analyst Ben Kepes will be building a Cloud Computing curriculum designed for technologists and non-technical users alike. The mission is to build widespread knowledge about the Cloud revolution and encourage discussion about the Cloud's benefits for businesses of all sizes. Read more CloudU whitepapers and register for upcoming webinars at www.rackspace.com/cloud/cloudU

Diversity Limited

Sponsored By: rackspace® HOSTING

Table of Contents

Executive Summary

One of the benefits of Cloud Computing that we have been articulating in this series of whitepapers is the benefit of abstracting responsibility for IT functions off to a third party. While this is indeed a benefit of Cloud Computing, it is important to realize that when it comes to security, customers still have a responsibility to ensure their data is secure.

Cloud Computing security should be regarded as a partnership between the vendor and the customer with both parties having responsibility for different aspects of security. In this whitepaper we detail the different aspects of security that need to be managed to ensure overall security in the Cloud. Moreover, we contrast those aspects of security that vendors are typically responsible for to those for which customers have an ongoing responsibility.

We contend that Cloud Computing is fundamentally more secure than traditional approaches but in order to ensure this security, some basic requirements must be met.

A Security Framework for the Cloud

The Cloud Security Alliance (CSA)[1] is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

Made up of subject matter experts from a variety of disciplines, and with chapters[2] all around the world, the CSA objectives are to;

- Promote a common level of understanding between the consumers and providers of Cloud Computing regarding the necessary security requirements and attestation of assurance.
- Promote independent research into best practices for Cloud Computing security.
- Launch awareness campaigns and educational programs on the appropriate uses of Cloud Computing and cloud security solutions.
- Create consensus lists of issues and guidance for cloud security assurance.

The CSA is focused on Cloud Computing security being a shared responsibility with both vendors and customers having a part to play. We support this contention and believe that neither party should be expected to be solely responsible for security in a Cloud Computing paradigm.

As with any partnership, it is important to clearly communicate up front the roles and responsibilities.

Before making a decision to go with any particular Cloud Computing vendor, ensure you have clarity on who does what as each vendor may be different. This paper does not describe the security practices of any particular vendor but rather a collection of practices that are typical across the Cloud Computing industry.

In a previous CloudU paper we took an in-depth look at the differences between the individual layers in the Cloud Computing stack[3]. In the case of SaaS, and to a lesser extent PaaS, the provider takes on much more responsibility for security and customers do not need to worry about virtual machine control, firewalls etc. This can be contrasted with IaaS where the customer has significantly more responsibility for security. Notwithstanding the differences between the various parts of Cloud Computing, we believe that all Cloud Computing customers should have a rudimentary understanding of the different aspects of Cloud Security.

Having explored a general security framework, the first aspect of Cloud security we will look at is what vendors can, and should, do.

What Vendors Should Do

As we detailed in a previous paper looking at the makeup of a modern Cloud Computing data center[4] there are numerous aspects that go into creating a robust and secure Cloud offering. We will begin from the outside and work our way inwards.

Physical Data Center Security

As we detailed in our IaaS report[5], physical security of the data center encompasses a number of different aspects. Briefly these are;

- Security of the building - Keycard protocols, biometric scanning protocols and round-the-clock interior and exterior surveillance should be a standard monitoring procedure for data centers
- Authorization of personnel - Only authorized data center personnel should be granted access credentials to data centers
- Background checking - Every potential data center employee should undergo multiple and thorough background security checks before they're hired

Vendors have a responsibility to ensure their data centers are highly secure as it is always easier to avoid a physical intrusion than it is to secure data once perimeter security has been breached.

Security of Host Machine Operating System

This aspect of security assumes an understanding of the difference between physical machines and virtual machines. For a grounding on the differences, a previous CloudU whitepaper[6] gives more detail but for the purposes of this paper, virtualization is the division of a single physical server into multiple "virtual" servers containing multiple sets of segregated data.

The operating system within which virtual machines are hosted requires extra scrutiny as it is the manager for guest virtual machines and hence any vulnerability within the base OS can have downstream impacts on the individual virtual machines.

This is logical as a vulnerability within any particular virtual machine will affect that machine only, to contrast, a vulnerability within the host operating system could give the attacker absolute access to all virtual machines on the same piece of hardware. Host machines should have extra protection including;

- An intrusion detection system
- The minimum number of user accounts possible
- Controls to limit administrator access to named accounts
- Strong/ complex access passwords
- No publicly accessible network accessible services
- Hardened systems running only the necessary programs, services, and drivers

Control of the Hypervisor

While, in most cases, control of individual virtual machines is the responsibility for the customer, vendors need to ensure robust security of the hypervisor itself, the tool which keeps the individual virtual machines separate.

Vendors should pay particular attention to the hypervisor as security breaches at this level can have major cascading effects. Particular attention should be made that vendors are using the latest production or stable version of their particular hypervisor and that security patches are applied quickly to maintain the integrity of the hypervisor layer.

Network Security

Network security consists of the policies and procedures adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources[7].

Network security, similar to other security aspects, consists of different levels of security. These include perimeter controls, controls to limit network access, and lists to regulate access control.

The Cloud Security Alliance has developed a Consensus Assessments Initiative as a form of research and assessment of vendors security controls[8]. It identifies several network level questions and readers should refer to the latest version of the document when performing due diligence on vendors.

Vendors have a critically important role in ensuring the security of Cloud Computing however, as we have stressed throughout this report, customers also have a part to play. It is to these customer focused requirements that we shall now turn.

What Customers Should Do

As mentioned previously the responsibility for ensuring Cloud Computing security doesn't solely rest on the vendor. Customers too have an important part to play in ensuring the security of the solutions they utilize. One of the most important protection mechanisms that customers need to know about is the firewall.

Firewalls

A firewall can be thought of as a protective system that sits between the local computer network and the Internet. The purpose of a firewall is to prevent the unauthorized access to the local computer by third parties using the Internet. Firewalls do this by analyzing traffic to and from the local network and securing unauthorized traffic.

As firewalls protect a customer's own local network, it is important to ensure that any local network connectable to the Internet includes strong firewall protection. Customers therefore need to understand the two types of firewalls that exist, hardware and software.

Hardware Firewalls

In the Cloud, hardware firewalls, which are frequently standalone servers or found built into broadband routers, are useful in that they tend to require very little set up and protect all machines on the local network. While hardware firewalls are relatively straightforward to set up and use, users should learn the specific features of their firewall to ensure it is configured correctly to guarantee optimum performance.

Software Firewalls

Software firewalls, unlike hardware firewalls that protect the entire network, are installed on individual machines and protect only the particular machine within which they are installed. Software firewalls focus on averting the possibility that a third party will gain access or control of the device. Because of the virtual nature of servers in a Cloud Computing scenario, typically software firewalls are the method best suited to protect a customer's virtual machine.

In addition to installing and maintaining a software firewall, another area that Cloud Computing users need to be aware of is patching and backups.

Patches and Backups

One of the benefits of Cloud Computing in general and Software as a Service in particular, is that it reduces the need for individual IT departments to perform routine tasks. Two of these routines tasks include patching and backups.

- Patching is the updating of software on individual devices with the latest version. This is important as software vendors generally roll out patches frequently to respond to security threats.
- Backups ensure access to data in the event of a loss of connectivity, service or primary data source. Generally backing up involves the copying of data from the primary location to some other locations so that, in the event of a loss, data can be restored rapidly

Cloud Computing customers should ascertain exactly what their vendor provides in terms of patching and backups, in many instances patching and backups of operating systems and applications is the sole responsibility of the customer. Many Cloud Computing users, regardless of the vendor's approach towards backups, utilize third party backup services to maintain alternative copies of their data. This strategy can provide another level of security in the event of a massive security breach at the vendor.

Customers also need to be aware that installing a local patch can potentially impact on the functioning of their Cloud Computing application. While this is unlikely to introduce security threats, it is a factor to consider and customers should ensure that any local patching does not introduce unintended issues.

One of the most important aspects of security, both in the Cloud and outside of the Cloud, is the need for strong passwords. This is the area to which we will now turn.

Passwords

The saying goes that technology is only as secure as the weakest link in the chain and often passwords are this weak link. There is little point in investing millions of dollars in security checks, firewalls, levels of physical security and the like only to have security breached by the use of an insecure password.

Users should follow several strategies when using passwords – complexity, expiration, differentiation, minimum requirements, and history.

- Complexity – Passwords should ideally include a combination of numbers, letters, both upper and lower case and special characters. Users should avoid passwords that are easily guessed (names, birthdates, the word 'password' etc)
- Expiration – Passwords should have an expiration date, beyond which they no longer work. 90 days is a typical expiration time. Passwords should be changed on an ongoing basis. Following this strategy makes it harder for hackers to gain illicit access to services.
- Differentiation – Users should chose different passwords for different services. Using one password for multiple services is a common cause of cascading security breaches. Using different passwords for every service by contrast can avoid security breaches affecting multiple services.
- Minimum requirements – Users should chose a password that meets some minimum criteria - for example passwords needing to be a minimum number of characters, include both alpha and numerical characters and upper and lower case letters
- History – Users shouldn't be able to select a password that is the same as their previous few passwords.

With secure and complex password, it is time to turn our attention to the security of individual virtual machines.

Security of the Virtual Machines

Vendors need to treat each virtual machine as if it were a separate physical server when it comes to security. Virtual machines share the same security vulnerabilities as physical machines and should be protected from the same problems; hardware failures, viruses, hacking, data corruption.

Best practices, as identified by the Center for Internet Security[9], with regards to virtual server security include;

- The firewalling of virtual machine layer service ports
- The use of encryption for communication
- Utilization of a hardened operating system for the VM
- The disconnection of unused devices
- The checking of file integrity
- The use of strong passwords
- The use of backups
- The use of Audit Logging
- The use of host based intrusion detection/prevention (IDS/IPS)
- The use of data encryption techniques (File/DB)

With the individual virtual machines secure, it is time to ensure nothing untoward happens when the device is connected to the Cloud.

Controlling Access to Devices Connected to the Cloud

Anytime a device is connected to the Cloud, it raises a potential vector for security breaches. We have already discussed how the use of software firewalls can avoid these nefarious uses, but customers also need to put in place physical and other controls to ensure that only legitimate internal parties are accessing Cloud systems.

Cloud Computing users, along with any IT users accessing a network, need to ensure that systems are set up to make illicit activity more difficult. Some actions an organization can take include;

- Physical Security – beyond the typical door locks and alarms, locking your desktop/laptop with a physical cable lock is very important especially when left unattended
- The use of password protected screen savers to ensure that an unmanned computer does not provide and easy way for illicit connection to the Cloud
- Computer Locking ensures that only users with the correct authorization are permitted to access particular network sites. Without the correct credentials the computer will disallow connection
- Rationalized access (often called Role Based Access) ensures that, rather than all users being able to access all services the organization uses, access

is needs based,

- an approach that sees users granted the minimum access needed to perform their jobs
- Administrators should ideally have the ability to remotely wipe stored passwords, bookmarks and other potentially sensitive information on a computer. In this way a lost or stolen machine is little more than an inconvenience rather than a real security threat
- Taking security of Smart Phones, PDA's, and Notepads into account especially when utilizing Cloud service provider's Mobile Applications.

If device access procedures are one line of defence, an even more important one is to ensure that the right people have access to devices from the start.

Ensuring the Security of Staff

Staffing issues do not just relate to Cloud Computing, they are a factor any time a worker may have access to sensitive information, valuable property or is in a customer facing role.

All potential employees should undergo a rigorous security check designed to weed out any personnel who may cause a security threat. Employees should continue to be monitored over time to ensure that this particular vector for security breaches remains watertight.

Summary

In this paper we have detailed a number of potential security risks from Cloud Computing (and computing in general) and we have detailed approaches that help to reduce these threats.

We reiterate that Cloud Computing security should be seen as a partnership between vendors and customers where both take responsibility for their own particular area. In maintaining this collaborative approach, Cloud Computing can and should be a significantly more secure way of delivering computing than traditional approaches.

But because each vendor may be different, care should be taken to understand the security approach of individual vendors and what areas of security they are responsible for.

About Diversity Analysis

Diversity Analysis is a broad spectrum consultancy specialising in SaaS, Cloud Computing and business strategy. Our research focuses on the trends in these areas with greater emphasis on technology, business strategies, mergers and acquisitions. The extensive experience of our analysts in the field and our closer interactions with both vendors and users of these technologies puts us in a unique position to understand their perspectives perfectly and, also, to offer our analysis to match their needs. Our Analysts take a deep dive into the latest technological developments in the above mentioned areas. This, in turn, helps our clients stay ahead of the competition by taking advantage of these newer technologies and, also, by understanding any pitfalls they have to avoid.

Our Offerings: We offer both analysis and consultancy in the areas related to SaaS and Cloud Computing. Our focus is on technology, business strategy, mergers and acquisitions. Our methodology is structured as follows:

- Research Alerts
- Research Briefings
- Whitepapers
- Case Studies

We also participate in various conferences and are available for vendor briefings through Telephone and/or Voice Over IP.

About Rackspace

Rackspace Hosting is the world's leading specialist in hosting and Cloud Computing. The San Antonio-based company provides Fanatical Support® to its customers, across a portfolio of IT services, including Managed Hosting and Cloud Computing. Rackspace is also the founder of OpenStack™, an open source cloud platform with broad industry support, designed to offer cloud consumers greater choice. For more information, visit www.rackspace.com.

About the Author

Ben Kepes

Ben is the founder and managing director of Diversity Limited, a consultancy specializing in Cloud Computing/SaaS, Collaboration, Business strategy and user-centric design. More information on Ben and Diversity Limited can be found at http://diversity.net.nz

Endnotes

[1] https://cloudsecurityalliance.org

[2] https://cloudsecurityalliance.org/Chapters.html

[3] http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-Cloud-Computing-Stack.pdf

[4] http://broadcast.rackspace.com/hosting_knowledge/whitepapers/SayGoodbyetoDIYDataCenters.pdf

[5] http://broadcast.rackspace.com/hosting_knowledge/whitepapers/SayGoodbyetoDIYDataCenters.pdf

[6] http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Revolution_Not_Evolution-Whitepaper.pdf

[7] http://en.wikipedia.org/wiki/Network_security

[8] https://cloudsecurityalliance.org/cai.html

[9] http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf