Stormy Skies: Security in Cloud Computing

David C. Shields

Submitted to Dr. Michael Hanners

In Partial Fulfillment of CSEC620

University of Maryland University College

Table of Contents

Stormy Skies: Security in Cloud Computing

Introduction

Cloud computing is a phenomenon that likely sounded much like science fiction when the concept was first discussed but that did not curtail technology companies from aiming to make it a reality. Humorously enough, the concept of cloud computing is very similar to the traditional AS/400 mainframe and thin client configurations popular in the mid 1990's only the mainframes became datacenters, the distances became greater, and the interfaces much more graphical. The concept of having a corporate-grade network with many of the same features of a large corporation yet at a fraction of the cost and manpower is quite an enticing option for companies both large and small as a way to reduce costs and optimize resources yet IT Security must be handled with the same granular analysis as a true corporate network would or the security of the data may suffer.

Reading the Radar: Assessing Vulnerabilities

As with any IT Security considerations, one of the first steps in determining the security of cloud computing is to assess the vulnerabilities inherent and implied with using such a technology. Cloud computing's virtualization is both a strength and weakness as the fact that none of the equipment is physically present at the office location prevents the need to defend those resources. Yet it makes it far too easy to forget that the cloud system is still dealing with data from the local office and any security considerations that would need to be implemented were the data in-house must still be implemented in some capacity at the cloud itself (Catteddu & Hogben, 2009, pp. 57-58).

The breadth and depth of specialized needs a company must consider in choosing cloud providers is far beyond the scope of this document but there are four key vulnerabilities that will be standardized across almost any organization's needs for securing cloud computing: data leakage, confidentiality breaches, loss of service, and audit trails.

Water Damage: Preventing Data Leakage

During a severe thunderstorm, it is not at all uncommon for a seemingly secure roof to somehow leak water into other houses from above. The amount of damage that a water leak could produce can vary depending on the size of the leak and what the water lands on. Ironically, the security infrastructure of a cloud computing environment bears a striking resemblance to the concept of a roof leak.

Arguably, the amount of risk for data leakage in a cloud environment would likely fall into a medium category (Catteddu & Hogben, 2009, p. 39). While the impact of such a breach is high in that it could potentially affect the reputation, trust, intellectual property, personal data and many other factors of an organization, the actual probability is only medium as the average cloud provider (if they want to be realistically considered by any notable companies) is likely to have taken many steps to ensure the security of the data they will be housing. Thusly, if the roof of the house was in good repair before the rain began to fall, it would be far less likely to develop a leak.

Nonetheless, if an attacker were to desire to target a company that was using a cloud provider for some (or all) of its data warehousing needs, the cloud would open a few particular ways that an attack could be rendered. The most notable item to an attacker is that cloud computing, by its nature, means that data must travel across the Internet at some point in time.

Data housed at an organization can be protected by whatever network infrastructure is in place at the location from which it originates and likewise will be protected by whatever infrastructure is in place on the receiving end at the cloud host's data center. An attacker is likely to see the effort to compromise data transmissions during the 'travel' time as an easier task then penetrating the actual networks from which they originate (Anthes, 2010, pp. 17-18). This gives rise to the possibility of man-in-the-middle attacks in an attempt to siphon data that is transmitted across the Internet using a tool like an SSL decryption engine. Furthermore, depending on the type of cloud service being used, some or all of the access tools may be linked to a web server that is open to any number of web attacks such as DDoS, SQL Injection, etc. Lastly, data could be leaked by the old standby, an insider who is motivated either by their own reasons or by outside influence to provide data to an unauthorized party (Choubey, Dubey, & Bhattacharjee, 2011, pp. 1229-1230).

To mitigate the risk of data in transit being compromised, both the customer and the cloud host must come to an agreement about the type of security mechanisms being used for the transmission of data including using SSL, SAML, XML signatures and various other means of identity validation (Reddy & Reddy, 2011, p. 7151). Managing the security controls from end to end to ensure compliance and infrastructure from leakage may prove to be much more challenging as there is a notable lack of standardization among cloud providers which means an organization needs to thoroughly evaluate their cloud provider to match their regulatory needs before agreeing on a contract (Anthes, 2010, p. 18). Although there is not tried and true way to determine whether or not the web server interface being used is secure and protected against attack, businesses that wish to move to cloud computing would be wise to research the technologies being used by their provider and make sure they have a thorough understanding of the known security vulnerabilities of the aforementioned technology as well as how the provider

plans to deal with incidents as they arise. Preventing the insider threat can be the most complicated to prevent because there is little that can be done to predict when an insider might 'turn' but if the cloud host performs background checks on its employees as well as having the employees sign specialized contracts if they must work with highly sensitive data, the chances of data being illegally offered to third parties may be somewhat stifled (Reddy & Reddy, 2011, p. 7152).

All in all, there are many policies and procedures that should be implemented to prevent data leakage but few of them would have much impact on the end users of the cloud services. In regards to securing communications, SSL is a freely available functionality of almost all modern web browsers so users would not find any impact from this need and may, in fact, feel more secure by knowing that the transmissions are secured by SSL (as evidenced by many notifications in the browser). There is certainly the possibility that users might be impacted by the availability to data and services during regularly scheduled update times but this will be easier to manage if the user is given notice of the planned outage times a great deal of time in advance as is common among many internet vendor websites. Furthermore, the time it takes for a business to select a cloud provider and/or receive updated background checks and required regulatory documents should have no impact on the user as this would be a procedure that would occur before a selection is made.

In fact, upper management of the organization in question may rightfully require access to the background checks and/or regulatory documents before they even permit the company to select a cloud provider.

Preventing data loss, much like preventing a leaky roof is a process that is best done proactively.

It is wise for any organization planning on using a cloud provider to gather documentation about all security measures available and to thoroughly analyze this information before agreeing to a contract. Taking steps such as verifying the security controls of the organization, the quality of workers managing the cloud, the regulatory requirements in place and the standard patching schedule will save a great deal of time and headaches for both the users and the management of the organization. The best way to reduce impact on the users and keep them happy is to be highly proactive in choosing and summarily auditing the cloud provider before selecting them and should be almost anticipated by any cloud provider offering such services.

Sandbagging for the Flood: Protecting Confidentiality in the Cloud

For anyone who has watched the news in recent years, there is no shortage of footage featuring flooded homes, banks of rivers swelling over with water, and people who spend every ounce of their energy putting up sandbags in the aftermath. However, in places such as Louisiana's Gulf Coast, areas right alongside the Mississippi River and many other places that have experienced the damage of flooding have usually prepared themselves ahead of time for the mighty power of the water they find themselves near. Much like the people who must be ever-diligent to protect their investment the next time the floods rise, businesses considering cloud computing should likewise prepare themselves when they are considering cloud computing. Information security professionals will be the first to warn that the question is not *if* an organization will have a data breach but *when* and using a cloud tenant brings on unique confidentiality issues in of itself (Anthes, 2010, p. 18).

The probability of a loss of confidentiality among cloud provider hosted data is considered to be high as it impacts everything from Critical Personal Data to Customer trust and service delivery all because of the very nature of the data itself (Catteddu & Hogben, 2009, p. 46). There are many different items that must be protected with great confidentiality including trade secrets, HR Data and countless other pieces of PII (Personally Identifiable Information) as many of the items in a conventional corporate network depend upon the protections a private network offers.

Much like the issue of preventing data leakage, the confidentiality of private information is only as well protected as the machines that house it and the people intended to take care of the equipment in the cloud where it resides. However, unlike the standard data one might be transmitting – such as an email or Office365 Word document – confidential data that might be stored on an Infrastructure as a Service (IaaS) server somewhere in the US is much more important to protect from unapproved parties (Sehgal, et al., 2011, p. 280). In cases such as this, it is critical that the hardware running on a virtual cloud management server must be configured in such a way as to enforce strict system autonomy and isolation as any cross-threaded process running on a different guest OS but on the same host could potentially open a path to the critical data (Anthes, 2010, p. 17). Again, the threat of the confidentiality of the data on a cloud could potentially be threatened by an insider but perhaps in an unintentional way. Almost any well managed IT Infrastructure requires various logging and health tests to judge the health of the servers and in a quality of service review, it is possible that a technician could accidentally read data that is confidential by simply pulling a random file for a system speed or integrity test.

To meet the demands of protecting data confidentiality, one of the most important steps is selecting the highest quality cloud provider for the price the organization is willing to elect.

One of the crucial steps in this process is selecting a provider with industry credibility which may take the form of reviewing the SOX compliance reports and SAS70 analysis, and any other standards auditing report (i.e. – NIST, ITIL, etc.). Although these reports do offer some insight into the company and its standards, they should not be considered a deciding factor in selection, merely as an additional identifier. It is also advisable to have a thorough understanding of the limitations of the contract between the business and the cloud provider – what is the statute of limitations in the event of a breach? Many of these concerns can be answered as the organization considers whom they wish to use as their cloud provider as they are obligated to set the proper expectations before agreeing to be a provider and is often known as the Service Level Agreement or SLA (Sehgal, et al., 2011, p. 282). Determining the types of data that may be reviewed by the datacenter technicians will likely prove more challenging as the various system health monitors may or may not be able to be used autonomously. The tools employed by the cloud datacenter administrators may also have to be set in a specialized way to prevent analysis of two separate guest systems at the same time, thus preventing seepage of data between hosts and a policy must be in place for this that complies with the organization's regulatory requirements (Ahmed, 2011, p. 12).

If the proper steps are taken, protecting the confidentiality of data in the cloud can be secured in a way that will not impact the user base at all. In fact, the evaluation of providers to determine SOX, SAS70, and any other regulatory requirements can be completed before the cloud is even implemented within an organization. It may be necessary for an organization to communicate with various business groups or employee groups to determine the exact requirements they may have.

This will be more likely to have a positive impact on the groups as they will not feel as though the process was forced upon them but rather that the actual workers were able to have an impact on the choices made instead of simply bending to the will of the management involved.

Power Outage: Recovering from Service Loss

By far, one of the most frightening and unsettling results of a strong storm is the loss of power to a home or business. Organizations invest in countless tools to prevent power failure including Uninterruptable Power Supplies (UPS), power generators, etc. in hopes to be able to keep their business running if the power is ever lost. If a powerful lightning bolt were to strike a transformer or debris damage a power line, the resulting loss of service could be unimaginable for some organizations. Yet in the case of a standard business, there are likely protective and preventative measures in place were a computing system or tool to lose service and the impact can be easier to manage since the technology is localized. However, in the case of a cloud system, the loss of service may be less manageable and certainly less expected.

The loss of service, surprisingly, is only considered a medium risk with cloud providers. Certainly, the impact of an outage could be decimating to certain business process but the cloud providers of any merit have built a strong amount of redundancy, thus resulting in low risk of service loss from the provider's end (Catteddu & Hogben, 2009, p. 31). A cloud computing center may experience connectivity issues in unexpected circumstances such as natural disasters but most providers will have additional network sources and power backup mechanisms that the loss of service is relatively unlikely (Anthes, 2010, p. 16). Despite the high availability of service offered by cloud providers, businesses must still exercise caution in assuming that all providers are created equal. While the provider may advertise high uptime, it is important to acquire additional information to validate those claims.

Furthermore, the loss of service may actually be trigged by the organization's network service provider rather than the cloud provider. As a result of this fact, the business should take additional steps to guarantee their own connections are reliable or risk a loss of service on their end.

The satisfaction of the customers using cloud services may be almost completely dependent upon availability of data. It is common for individuals to resist change and in the event of a change the users will be more likely to perceive it as the reason for a problem even if the two items are unrelated. Modern businesses depend upon 24x7 availability of critical data to meet the needs of their organization and may or may not be accepting of 'expected' downtime that might be required to restore order to a cloud data source. Businesses that intend to use cloud computing would be wise to supply secondary connection interfaces to the cloud provider and may even require cloud providers to offer secondary or 'redundant' servers for critical applications (Reddy & Reddy, 2011, p. 7153). In most cases, the cloud providers will craft an SLA that guarantees a specified amount of uptime for a specific application or even the infrastructure as a whole and will usually offer a financial or other compensatory measure in the event of a violation of that agreement (Sehgal, et al., 2011, p. 281).

Conclusion

Despite the risks of using a cloud service (both perceived and realistic), the solution offers a considerable number of benefits to the companies willing to use them. These benefits include less management overhead in technology and infrastructure, lower power consumption for the office of the business, and much higher uptime than may be possible for a smaller organization (Anthes, 2010, p. 16).

The secret to forging a secure and dependable partnership between a business and the cloud provider is to take considerable amount of time to evaluate the needs of the business as well as the offerings of the cloud providers and come up with a partner that will supply the best fit for the needs of the organization while still remaining within regulatory compliance. If the user base within the company is given a voice in the selection and the proper concessions are made to meet the needs they express, the relationship will be a happy and helpful one for all parties involved. As the technology progresses, so will the needs of the business and with proper security controls in place, cloud computing can offer a scalable, valuable service for a lower total cost.

Bibliography

Ahmed, A. (2011, April). Using COBIT to Manage the Benefits, Risks, and Security of Outsourcing Cloud Computing. *Information Systems Audits and Control Association, 2*, 12-16.

Anthes, G. (2010, November). Security in the Cloud. *Communications of the ACM, 53*(11), 14-18. doi:10.1145/1839676.1839683

Catteddu, D., & Hogben, G. (2009). *Cloud Computing: Benefits, risks and reccomendations for information security.* Heraklion: European Network and Information Security Association.

Choubey, R., Dubey, R., & Bhattacharjee, J. (2011, March). A Survey on Cloud Computing Security, Challenges and Threats. *International Journal on Computer Science and Engineering (IJSCE), 3*(3), 1227-1231.

Reddy, V. K., & Reddy, L. S. (2011, September). Security Architecture of Cloud Computing. *International Journal of Engineering Science and Technology, 3*(9), 7149-7155.

Sehgal, N. K., Sohoni, S., Xiong, Y., Fritz, D., Mulia, W., & Acken, J. M. (2011, Jul-Aug). A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing. *IETE Technical Review, 28*(4), 279-291.