Cloud Computing Secured

Thomas Mitchell CISSP

A Technical Communication
Abstract

With the migration to Cloud Computing underway in many organizations’ IT infrastructure, this will cause a paradigm shift into Endpoint Security. The migration to Cloud Computing will start an evolution and product shift for the traditional security vendors.

The will have to adapt their existing security portfolios into cloud based offerings for Endpoint Security. Let us examine and see what we will need to have to secure us from the vulnerabilities that this will bring to our infrastructure.

But let us first take look at Cloud Computing and let’s see what it is.
# Table of Contents

- What is Cloud Computing .......................................................... 4
- Public or Private Cloud ............................................................ 5
- Cloud Computing Pros and Cons .............................................. 10
- Cloud Computing Bright Future ............................................... 11
- References ................................................................................ 13
What is Cloud Computing

Cloud Computing is a general term for anything that involves delivering hosted services over the Internet. The name Cloud Computing was inspired by the cloud symbol that's often used to represent the Internet in flow charts and diagrams.

Hosted services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The companies that have been in at this are household names such as Open Air, Sales Force.

Online retailers such as Ebay and, Amazon along with big box retailers like Wal-mart provide Cloud Computing services. For PaaS, Microsoft and Google Docs offer services. There are many household names invested in this technology. Cloud Computing.

A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is dynamic by design, a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider as the consumer needs nothing but a personal computer and Internet access.

Significant innovations in virtualization and distributed computing as well as improved access to high-speed Internet and a weak economy have accelerated interest in Cloud Computing. I predict that Cloud Computing will explode within the next 18 months specifically because of the economy and the need to stretch already tightened budgets.
Public or Private Cloud

A cloud can be private or public. A public cloud sells services to anyone on the Internet. Amazon Web Services today is the largest public cloud provider.

A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of Cloud Computing is to provide easy, scalable access to computing resources and IT services.

Cloud Computing Here are some implementations of public and private Cloud Computing that are household names such as internet email providers such as Google mail and Yahoo Mail; photo sharing sites such as Snapfish; video sharing sites such as You Tube; online backup like Mozy; social networking sites like Facebook, Linkedin and Plaxo stock trading sites such as E-Trade, Fidelity; and tax preparation giants like H&R Block and Jackson Hewitt.
Cloud Computing Security

First, let us address the seven deadly security sins that it may effect the traditional corporate network using Cloud Computing which are outlined below. The primary concern addressed is privileged access control. I will discuss what happens when a user requests access to resources and applications that are not in the company’s physical control. The user will need to have access to certain applications and data sources to carry out job functions. Called cloud control, with access similar to AD Group Policy Objects, it should be maintained and operated by the company that has requested the service even though the data is being physically hosted and housed someplace else. The “where is my data” comes into reality since the organization has outsourced applications outsourced storage and occasionally outsourced the outsourcer.

As previously mentioned, let us define these seven sins of Cloud Computing:

1.) Privileged User Access: End Users having enough access to enable them to accomplish their respective jobs and no more. For example, if your job is in the Finance department then you would have a need to have access to Finance applications and the Finance department’s database. However, you would not need to have a need to have privilege user access to the Human Resources database and associated applications as that is not your department. Role-based cloud authentication can take on a whole new meaning and implementation.

2.) Regulatory Compliance: Laws and Regulations that are mandated by a government entity that a company must adhere to if they are governed by that entity. These laws and regulations can have a monetary or civil or criminal penalty if they are disregarded or not adhered to giving an inherent incentive to
adhere to regulatory compliance.

3.) Cloud Location: Where is my data located? Well with the advent of Cloud Computing this answer may very well be Boise, Idaho or Punjab, India. The data location can be very complicated as to the exact location for purposes of accountability. The service providers may use a number of other service providers and the lines may blur to exactly where at the data is. This poses a problem for a host of Regulatory compliance issues. So similar to the data cloud may be moving and to find out where it is physically could pose a challenge. Knowing where your data is at is fundamental for security.

4.) Cloud Segregation: With cloud services you really do not know where your data is. This will cause nightmares for your risk management officer. Data in the cloud is typically in a shared environment alongside data from other clients. The Data can be com mingled with other customers where the data stored is. Companies should ask what other companies are storing information in the cloud.

5.) Cloud Storage and Recovery: This offers an alternative to using on-site tape or disk backup as a secure data recovery resource. The location of the storage will impact the mean time to recovery. As a best practice you could have a combination of cloud applications that talk to both local systems where the data resides, at the company and in the cloud.

6.) Cloud Forensics Investigations: If a forensics investigation is required, Cloud Computing could pose a challenge. Previously, you could seize equipment and get your hands on actual data. With Cloud Computing this becomes a challenge because of the dynamic nature of the cloud. You may start one track and end up.
Organizations may want to implement contractual assurance with the service provider that if you need to conduct forensics operations that you could obtain it easily. If the service provider is hesitant to guarantee this upfront, then assume that you will not be able to accomplish it later.

7.) Cloud Performance: Many cloud providers don’t provide service level agreements (SLAs) guaranteeing uptime and the SLAs that are available provide meaningless compensation in case of outages. Also let us not forget about network uptime when determining cloud availability. The Cloud Computing challenge is that there should never be any down time if the implementation is done properly. If Cloud Computing stops so has the Internet. This is what the vendors of Cloud Computing services tout as service availability. They are always available.  As you can see there are different yet similar security vulnerabilities that expose proprietary data systems and intellectual properties to the rest of cyberspace. While using Cloud Computing gives us advantages it also brings organizations challenges in how to secure it.

The virtualization of application and data sources is sexy and cost effective; this also should raise red flags about having more controls not less for the end user. While the current suite of desktop security products. The desktop security products that feature the product line of Anti-virus, Anti-Spam, Firewall, Host Intrusion Prevention, Compliance Auditing, Data Loss Prevention, Data in Motion Encryption is being deployed to assess protect and control assess endpoint desktops and mobile devices.

The host intrusion prevention being deployed should be configured to work seamlessly with cloud control access. The Cloud Computing has an access control list
ACL’s with the Cloud Control should also work together with the all of the products that have been rolled out to protect the desktop and the level of access will be determined by the Group Policy Object (GPO) located within the directory domain structure type object that the end user is in.

Another concern is the development of a tight access and control architecture. As the web services can be reached from anywhere, restrictions need to be placed on how the information is accessed. Role or rule-based access could easily solve these challenges.

Role and rule-based applications are integral in the development of a Cloud structure as clouds tend to form over and over again. This makes the cloud vulnerable to passing customers that may share the same cloud. What you want to look for in a solution is a seamless and unified security solution. You should want to look for a cloud service to protect.

I would suggest that you look for a Software as a Service (SaaS) offering when looking for Cloud Computing Company. This type is already designed and developed primarily for providing protection, also called Cloud Coverage Secured.
Cloud Computing Pros and Cons

From a business perspective there are many pros to Cloud Computing as we have read. The businesses that are already involved in Cloud Computing speak volumes of the promise that is being delivered today. The mainstream business person is waking up and taking a good hard look at what it can bring to their business and bottom line. The current and future outlook of the economic market place makes this a good alternative to owning additional hardware and software and adding personnel. The cost cutting savings of utilizing cloud services can translate into reinvestment back into the building and expanding the business.

The cons on the other hand are not as obvious. The cloud concept leaves you with an ill feeling when you start to think of the bad side. If there was a breach could you find its origin? If there is a virus outbreak pinpointing the source and stopping it within a day could be difficult. Where is my data stored in Canada, Iceland, India, China and so on? Or, you may have a customer that wants their data stored in the U.S. because of regulatory compliance issues. With Cloud storage, one may not be able to guarantee this. Thus, we may create a new source of litigation. Just imagine what type of Service Level Agreements (SLA) agreements you will have to create to support this new business model agreement.
Cloud Computing Bright Future

The future of Cloud Computing is rapidly changing at the writing of this article. I will highlight some of the advancements of Cloud Computing.

Hewlett-Packard announced its ePrint platform and a line of printers that will print documents or files directly from the cloud. Users simply send a Web page or a document to an e-mail address associated with the printer and the receiving printer or all-in-one device then prints out the material. Documents or files can be stored in the cloud and printed when needed.

Panda Software announced the release of Panda Cloud Antivirus Pro, a cloud-based antivirus service, with accompanying support. The security company also updated its free Panda Cloud Antivirus software, first introduced in April 2009, which offers a subset of the Pro version's features. New features in both versions include a dynamic behavioral blocker which helps spot and block malware -- even if it's not previously been seen -- as well as targeted attacks. The Pro version also includes automatic upgrades and automatic scans of USB drives and hard drives to ensure they can't introduce a virus even if the machine is offline. Multilingual technical support is available via an online forum.

These are two recent announcements tells you that Cloud Computing is here to stay. HP's announcement makes Cloud Computing more cost effective. You do not have to buy or rent a printer. There will be many more services in the cloud offering to make a business think long and hard about spending capital on traditional infrastructure. Business owners can rent an address and lease space in a building for meetings by the hour. Your business can be totally ran in the cloud.
This is the promise and the offering that Cloud Computing brings a paradigm shift for the 21st Century business to move on to the new business model. The government Cloud Computing development is already underway. The cloud movement is strong, growing and becoming more accessible and economically sound as a new business model.
References


http://www.themanufacturer.com/uk/content/10126/Demystifying_the_cloud

http://www.alliedindia.com/cloud-computing.html

http://www.informationweek.com/news/hardware/peripherals/showArticle.jhtml?articleID=225500020&cid=nl_IW_cloud_2010-06-09_h