

Cyber Securities on Cloud Company Systems

Speakers:

Prof. Yoshiaki Fukazawa, Senior Executive Director for Research Promotion and IT Promotion, Waseda University

Mr. Jeb Linton, Strategy Exec. IT Architect, Cloud Computing Strategy, IBM CHQ

Abstract

Cloud based computing has become a very popular method to access resource on the Internet because it is economical and more efficient. Cloud based computing has the ability to facilitate the exchange of information among a large quantity of servers without any problems of over usage. Since cloud computing has become more popular concern has grown as to how to secure the information stored within cloud-based systems. This discussion focused on methods to secure cloud computing so we can continue to utilize it.

Summary

Prof. Yoshiaki Fukazawa.

Prof. Fukazawa began his presentation providing an overview of cloud computing and how it has grown in the last five to six years. Originally Prof. Fukazawa had a difficult time understanding cloud computing because in the beginning it seemed to just be a “buzz” word. Cloud computing was always talked about in general terms as an alternative to hardware server providers. As cloud computing has developed over the years Prof. Fukazawa commented that he has now learned to have appreciation for it.

Prof. Fukazawa further explain the intricacies of cloud computing and how it is generally used today. Cloud computing is a method which allows a pooling of resources to be accessible to an abundant amount of users. The resource pooling is not dependent on location and can be accessed from mobile devices such as computers, laptops and smart phones. The Internet serves as a host to the pooling of resources but since it is not location dependent there is rapid elasticity and on-demand self-service. The provider of the resource pool can dynamically manage it according to the demands of the consumer. The concern is the consumer does not know where the resource is coming from. The resource itself can be monitored and controlled when provided to the consumer.

Cloud computing has three service models, software service, platform service and infrastructure service. The software service allows the capability of the user to use the provided applications running on the cloud infrastructure. The platform service is the capability to deploy on the cloud infrastructure using programming run agents supported by the provider. The last one is the infrastructure service; this allows the consumer to learn operating systems and applications. The deployment methods are broken down into four categories, private cloud, community cloud, public cloud and hybrid cloud. Private clouds are used and manage by one particular user.

Community clouds are created for an exclusive use by a specific community of users. The public clouds are clouds provided for the general use of the public and are not specific to one particular group of users. The last form of deployment is the hybrid cloud that allows two forms of deployment to be combined.

Prof. Fukazawa expanded upon the current cloud system at Waseda University and how it is secured. Currently Waseda is dependent upon a great amount of unix-based servers. The goal of Waseda University is to transition out of using unix-based servers into using only cloud servers. Cloud computing would only require 45 servers versus the current 223 Waseda used in 2010. By using cloud Waseda will meet the demands of using less energy and provide better service to a greater amount of users. To secure the Waseda based Cloud, Waseda has the ability to set up its own restraints to regulate who can access the cloud and the information within it. Since Waseda is able to control its own cloud services it can provide a great deal of security for its users and the information protected in the cloud.

After explaining the benefits in cloud computing Prof. Fukazawa shared his own concerns with cloud computing. In terms of reliability cloud computing is heavily dependent on the Internet as a host and a method for users to access it. Cloud computing also does not eliminate the problem of needing large-scale servers to provide the infrastructure of hosting the information. In terms of security there is a concern of location independence. Users are not aware of where the information is coming from or who is providing the information. There is also a concern of user privacy because although information can be protected in the cloud it is difficult to protect the information of the users. Prof. Fukazawa then commented on a quote in a recent news paper publication that google plans to track users across all of its sites. This means google will have the ability to gather more information about its users than the user would be inclined to give. As cloud computing becomes more popular everyday these problems will become more important in ensuring safe cloud based computing.

Mr. Jeb Linton

Mr. Linton began his remarks stating that cloud computing is an emerging paradigm in computing and with each new method has the concern of security. As cloud computing becomes more enhanced security must evolve to meet the risks posed by cloud computing. The biggest inhibitor to cloud computing today is the risk posed by its usage. While it is considered to be an effective tool in sharing a resource of information many are concerned with how safe it actually is in securing a pool of resources. This happens whenever you have an infrastructure that is shared. The level of complexity of identity control is magnified. The ability to federate identity and access control becomes more important. To gain the trust of organizations cloud services must deliver security and privacy expectations that meet what is available in traditional IT environments.

When securing cloud-based infrastructures it must be taken into consideration exactly why kind of information is being secured. Depending on the information provided in the resource pool will depend on how best to secure that information. When you are

dealing with medical information verses government information security on how to govern this information will vary. Security will also vary depending on what kind of cloud you are dealing with. When working with a private cloud the security controls will be much easier to specify in comparison to a public cloud. If you have a fully public cloud there is less ability to customized security controls. In general the same rules apply, in general you have the same range of security controls that need to be considered. All businesses that work with cloud computing today have experience in dealing with this kind of security. The key is to build in security to every layer of the cloud infrastructure. The same essential concerns apply to all forms of services provided within the cloud from software services to infrastructure services.

The important thing to remember is that framework for the security depends on the company but each cloud has a typical security framework. This framework is a foundational set of security controls but they need to be reapplied depending on the particular needs of the cloud implementation. This has to take place throughout the life cycle of the implementation. The first phase is to establish a cloud strategy and implementation plan. Following this you want to deploy your strategy when building your cloud services. Finally you want to manage and optimize the consumption of cloud services. In other words govern the cloud through ongoing security operations. As you build and grow your cloud you want to be thinking about security at every level.

The type of cloud being implemented will have particular areas of focus. When building an infrastructure you need to focus on managing datacenter identities, monitor logs on all resources and defend network threats. Platform service will require a security focus in pre-built, pre-integrated IT infrastructures tuned to application specific needs. When in the process of becoming a cloud provider you need to have an advanced platform for creating, managing and monetizing cloud services. The key thing to remember is that with each service there will need to be a unique set of security applications.

There are a number of advance technologies that Mr. Linton at IBM is working on to help make cloud computing more secure. IBM has the largest, most complete IT security portfolio across the domains in the IBM security framework. The main thought Mr. Linton wanted to leave us with was that as new technology advances security must advance as well to meet the demands of the consumer. Security analytics is a constant ongoing project and as new challenges are brought forward we must always look for ways to meet them.