*Michigan Information Sharing and Analysis Center*
*Monthly Cyber Security Tips*

# *NEWSLETTER*

*April 2010* Volume 5, Issue 4

## Cloud Computing

### What is Cloud Computing?

Cloud computing is a growing trend in information technology as organizations look for ways to save money and add flexibility to their operations. Cloud computing, while still an evolving service, provides on-demand network access to a shared pool of computing resources such as networks, servers, storage and applications. The pooling of resources allows the provider to rapidly scale to meet changing customer demands. The service is typically provided through a large data center. Cloud computing can be divided into three types: Software as Service, Platform as Service, and Infrastructure as Service.

- ***Software as a Service (SaaS):*** Provides ready for use web-based applications such as email that are maintained centrally by a provider (e.g., Gmail, Salesforce.com).
- ***Platform as a Service (PaaS)*:** Provides programming languages and tools that can be used by application developers to create and deploy applications on the web.
- ***Infrastructure as a Service (IaaS)*:** Provides computing resources, such as virtualized servers and storage, whose usage is rented from a provider (e.g., Amazon EC2, Windows Azure).

In addition, cloud computing can be private, available for a single organization/group of users, open to the public, or some combination of these models.[1]

The growth in cloud computing is fueled by economies of scale. Cloud computing allows users to pay for what they need, when they need it.

### What are the Security Concerns with Cloud Computing?

There are security and privacy concerns that must be considered before moving to cloud computing, including the following:

- **Vendor Security**: Cloud computing customers rely on providers to implement appropriate security measures to protect the confidentiality, integrity, and availability of data. Be wary of providers who are reluctant to share details of their security architecture/practices with customers.
- **Isolation/Segregation**: Users access cloud computing resources via a virtual machine hosted on an unknown physical machine[2]. The physical machine may be shared with other users. Providers must ensure that multiple customers do not interfere with each other, maliciously or unintentionally.
- **Data Location**: Providers may have data centers located in other countries. Be sure your vendor contract stipulates any restrictions you may have on the physical location of where your data is stored.

- **Management Interface**: Customers access the cloud management interface via the Internet, thus increasing exposure to potential attack.
- **Reputation Sharing**: Bad behavior by one cloud customer may impact others using the cloud. For example a customer engaging in spamming may cause a common cloud IP address to be blacklisted.
- **Provider Viability**: What happens to your organization's applications and data in the event that the provider goes out of business?
- **Compliance**: Placement of data in the cloud does not eliminate an organization's need to meet legal and regulatory requirements such as PCI or HIPAA. Organizations will need timely assistance from cloud computing providers to fulfill investigation/audit requirements.

## What Should Organizations Do?

Organizations should fully research the risks and benefits of cloud computing before moving to that environment. It is critical that security requirements are addressed in contractual agreements in advance. In addition, there are steps organizations should take when using cloud computing:

- **Data Classification**: Consider the sensitivity of your data before making a decision of whether or not to put it in the cloud.
- **Encryption**: Encrypt sensitive data before placing it in the cloud.
- **Authentication:** Consider requiring multifactor authentication for access to cloud computing resources.
- **Vulnerability Assessment**: Include a requirement for a security review or vulnerability assessment as part of the service level agreement with the provider.
- **Monitor**: Require close monitoring of cloud computing resources by providers for unauthorized activity.
- **Backup:** Ensure that your backup data is not comingled with other customers.
- **Notification**: Require providers to provide timely notification of any potential data security breach.

## Additional Information:

[1] The NIST Definition of Cloud Computing. October 2009. http://csrc.nist.gov/groups/SNS/cloud-computing/

[2] D. Hilley. Cloud Computing: A Taxonomy of Platform and Infrastructure-level Offerings. April 2009. http://www.cercs.gatech.edu/tech-reports/tr2009/git-cercs-09-13.pdf

**Cloud Security Alliance:** http://www.cloudsecurityalliance.org/
M. Armbrust et al. Above the Clouds: A Berkeley View of Cloud Computing. February 2009.

**For more monthly cyber security newsletter tips visit:** www.msisac.org/awareness/news/

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.*

***Brought to you by:***

MS-ISAC