

Information Assurance for Systems Deployed in Cloud Computing Environments

Cloud computing provides many advantages to organizations looking to maximize their IT expenditures while minimizing their physical footprint. While the gains are easily understood in terms of server maintenance, management overhead, and time to market – what are the security implications of moving into the cloud? Does your organization understand their access rights to the computing infrastructure and more importantly your data? The cloud can offer a significant benefit. However, it is of paramount importance that an organization act with due diligence to ensure that their needs can be met by their selected cloud provider. The Falkland Group can help your organization navigate the ins and outs of virtualization to ensure your data stays safe and secure in the cloud.

Definition of Cloud Computing

The cloud computing model as defined by the National Institute of Standards and Technology (NIST) comprises five essential characteristics (1):

On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity - Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

The NIST definition of cloud computing includes three service models:

Cloud Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS) - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

The NIST definition recognizes four different deployment models for cloud computing environments:

Private cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud - The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Cloud Security Threats

Threats in the cloud environment can be broadly categorized into two groups, threats due to the consumer's relationship with the cloud service provider, and threats due to the technology used to host the cloud. Threats of the first type arise from the cloud provider sharing duties that the information system (IS) owner would traditionally have held sole responsibility for. These challenges are similar to those previously presented by outsourcing or hosting, in general they need to be addressed by transparency on the part of the cloud service provider and by well-written contracts and service-level agreements. Threats of the second type arise from the technologies underpinning the cloud infrastructure,

The Cloud Security Alliance (CSA) and the European Network and Information Security Agency (ENISA) have highlighted the following threats to cloud security (2)(3)(4):

Abuse and Nefarious Use of Cloud Computing - Examples include spammers using cloud services resulting in blocks of cloud IP addresses being blacklisted, shared resources being seized when a co-tenant is subpoenaed, malicious probing/scanning, and network mapping such as that demonstrated by Ristenpert et al (5).

Insecure Interfaces and APIs - Vulnerabilities in the interfaces used to provision, manage, and monitor cloud resources; these interfaces are typically Internet accessible. This type of vulnerability could potentially affect multiple virtual machines or the overall cloud system.

Malicious Insiders - For example, a cloud provider may not apply the same hiring standards as the cloud consumer, resulting in an increased insider threat risk.

Shared Technology Issues - This threat type includes guest-hopping attacks, and attacks against hypervisors such as Kostya Kortchinsky's CloudBurst (6). As cloud resources are allocated based on statistical prediction there is the possibility of resource exhaustion, in some cases resulting in a fail-open state.

Data Loss or Leakage - Potential for data leakage during inter- and intra-cloud transfer. Inadequate data deletion when resources are reallocated, data wiping may not be possible through the service's API.

Account or Service Hijacking - A threat not specific to cloud systems, but exploitation in a cloud environment potentially has wider-ranging impact.

Unknown Risk Profile - This threat arises from insufficient knowledge about the service provider's security practices and policies. Lack of information about the provider's log review policies, software versions etc. can result in the consumer inaccurately calculating their security posture.

C&A of Cloud Systems

When accrediting an IS deployed to a cloud computing environment the accreditation boundary and responsibility for the controls being evaluated will be determined in part by the deployment model and service model used by the cloud. For example, under a SaaS service model a greater number of controls would be the responsibility of the cloud service provider than in an IaaS service model. Inheritance of controls between the cloud service provider and the consumer/IS owner needs to be clearly established. The cloud service provider's resources will need to be certified in addition to the ISs residing in the cloud, this can be complicated if the provider can not provide evidence of compliance or if it does not permit audit by the consumer.

Current Picture of Accredited Clouds

The DISA Rapid Access Computing Environment (RACE) is a community cloud that offers PaaS via Virtual Operating Environments (VOEs) deployed to development, test, and production zones. The VOEs are provided pre-hardened with applicable Secure Technical Implementation Guides (STIGs). Once provisioned, responsibility for maintaining the compliance of the VOE falls to the client (7).

Google Apps for Government is a community cloud offering SaaS applications for email and collaboration. Google Apps for Government received a Federal Information Security Management Act (FISMA) accreditation from the General Services Administration (GSA) in JUL2010 (8).

Microsoft's cloud computing infrastructure received FISMA accreditation in DEC2010. Two of Microsoft's SaaS products, Exchange Online and SharePoint Online, are currently in the process of obtaining FISMA accreditation (9).

Eleven other vendors have a Blanket Purchase Agreement from the GSA allowing them to sell their IaaS offerings through the apps.gov portal, however they have yet to be FISMA accredited (10).

References

1. NIST. "The NIST Definition of Cloud Computing."
<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>
2. CSA. "Security Guidance for Critical Areas of Focus in Cloud Computing." V2.1

<https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>

3. CSA. "Top Threats to Cloud Computing." V1.0

<https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>

4. ENISA. "Cloud Computing - Benefits, risks and recommendations for information security."

<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>

5. Ristenpart, Thomas, Eran Tromer, Hovav Shacham, Stefan Savage. "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds."

<http://people.csail.mit.edu/tromer/papers/cloudsec.pdf>

6. Kortchinsky, Kostya. "CLOUDBURST - A VMware Guest to Host Escape Story."

<http://www.immunityinc.com/downloads/cloudburst.pdf>

7. Sienkiewicz, Henry J. "DOD & Cloud Computing: Rapid Access Computing Environment(RACE) – A Case Study."

http://semanticcommunity.info/@api/deki/files/4578/=Henry_Sienkiewicz12092009.pdf

8. Krishnan, Kripa. "Introducing Google Apps for Government." The Official Google Blog

<http://googleblog.blogspot.com/2010/07/introducing-google-apps-for-government.html>

9. Thomas-Flynn, Gail. "Microsoft cloud receives FISMA approval." Bright Side of Government blog

http://www.microsoft.com/industry/government/state/brightside/detailBlog.aspx?title=Microsoft_cloud_receives_FISMA_approval

10. Wali, Sahar. "Cloud-Based Infrastructure as a Service Comes to Government." US General Services Administration Website

<http://www.gsa.gov/portal/content/193441>