Interested in learning more about security?

SANS Institute InfoSec Reading Room

An Introduction To Securing a Cloud Environment

While Cloud services offer flexibility, scalability and economies of scale, there have been commensurate concerns about security. As more data moves from centrally located server storage to the Cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at risk if appropriate measures are not put in place prior to selecting a Cloud vendor or implementing your own cloud and migrating to Cloud services. Cloud services such as Software as a s...

This is a GIAC Gold Template

An Introduction

To Securing a Cloud Environment

GIAC (GSEC) Gold Certification

Author: Todd Steiner, tsteiner@innd.uscourts.gov
Advisor: Hamed Khiabani

Accepted:

Abstract

While Cloud services offer flexibility, scalability and economies of scale, there have been commensurate concerns about security. As more data moves from centrally located server storage to the Cloud, the potential for personal and private data to be compromised will increase. Confidentiality, availability and integrity of data are at risk if appropriate measures are not put in place prior to selecting a Cloud vendor or implementing your own cloud and migrating to Cloud services. Cloud services such as Software as a service, Platform as a service or Infrastructure as a service will each have their own security concerns that need to be addressed. This paper reviews the best practices to secure Cloud services and data, including conventional security techniques and working with vendors to ensure proper Service Level Agreements exist.

[VERSION June 2012]

1. Introduction

As government and private industry budgets continue to shrink, executives are plotting new strategies to become more efficient and cost effective. Cloud computing has gleaned a lot of attention over the past several years as a means to reduce IT expenditures, improve scalability and reduce administration over head. The General Service Administration (GSA) has recently announced they have achieved a cost savings of almost $2 million dollars a year since migrating from Lotus Notes to Google's Cloud based email (Coleman, 2012). The savings includes cyclical replacement hardware, licensing and maintenance costs, thereby effectively reducing their total cost of ownership. Traditional server farms can now be replaced with centrally hosted virtual servers that can be managed by a fraction of people. According to Gartner, the typical IT organization invests two-thirds of its budget to daily operations. Moving to the cloud will free up 35 to 50 percent of operational and infrastructure resources (Wilcox, 2011). As savings mount and as efficiencies increase, Cloud computing will continue to grow. Through 2015 Chief Information Officers expect to operate the majority of their applications or infrastructure in a Cloud environment (McDonald, 2011).

Delivering IT services via the Cloud portends to be a time saver, a money saver and allow for better efficiencies. This is achieved primarily by leveraging the capacity of a data center. Google and Amazon are two widely known data centers providing Cloud computing and storage. Software such as VMware has enabled business to create a privately owned Cloud. Along with the gains achieved in Cloud computing there are inherent security risks.

1.1. Definition of Cloud Computing

The National Institute of Standards and Technology has defined Cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell & Grance, 2011, p. 2).

NIST categorizes Cloud computing into a Service Model and a Deployment Model. The Service Model consists of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). This "stack" of functionality begins with Infrastructure as a Service where consumers utilize hardware only. Moving up the stack is Platform as a Service. This layer offers the consumer an application environment

where programming libraries and software can be used for development. At the top of the stack is Software as a Service. The consumer utilizes the Cloud providers' application and has no access to the infrastructure or Operating System platform.

NIST Deployment Model consists of:

Private Cloud: The infrastructure is provisioned for exclusive use by a single organization.

Public Cloud: The infrastructure is provisioned for open use by the general public.

Hybrid Cloud: The infrastructure is a composition of two or more distinct cloud Infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

Community Cloud: The infrastructure is provisioned for exclusive use by a specific community of consumers who have shared concerns.

NIST also defines five key characteristics of a Cloud environment: Measured Service, Elasticity, Resource Pooling, On Demand Self Service and Broad Network Access. NIST's five essential characteristics, three service models and four deployment models are shown in Figure 1.

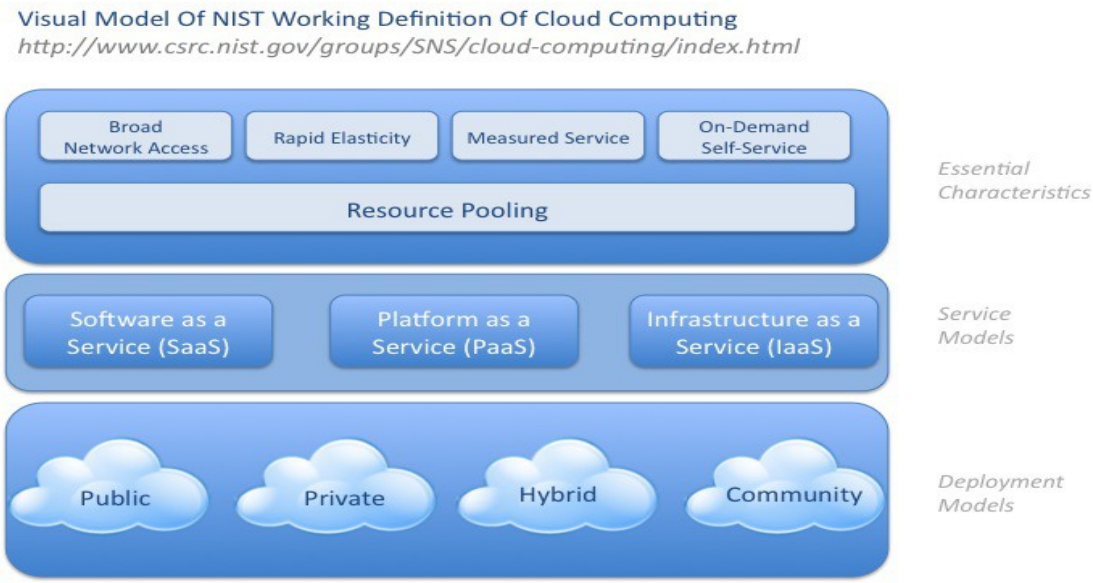

Figure 1

2. Cloud Infrastructure

2.1. Virtualization and the Cloud

A key component of Cloud computing is virtualization. While Cloud computing is not equivalent to virtualization, virtualization technology is heavily used to operate a Cloud environment. According to Ottenheimer and Wallace, "Virtualization is the creation of virtual resources from physical resources." (Ottenheimer and Wallace, 2012, p. 1). In a virtual environment, one host that previously ran a single Operating System now has the ability to run multiple guest operating systems as virtual machines. Virtual machines can be created quickly and easily in a Cloud environment. The infrastructure is invisible or abstracted from the consumer. The hypervisor is the software that manages communications between the physical server's memory, CPU or processing capability and the virtual machines that are running. The hypervisor allows virtual machines to be quickly provisioned or decommissioned. VMware, Microsoft HyperV and Citrix XenServer are commercial products to create a virtual computing environment. The down side to this virtual world is an increased opportunity for hackers to exploit vulnerabilities. The attack surface has increased because vulnerabilities may not only exist in the physical equipment but vulnerabilities may exist in the virtualized environment (virtual NICS and virtual switches).

The lower down the stack you go, the more security the consumer is responsible for. In SaaS environments the Cloud service provider is responsible for security controls. In an IaaS environment, the Cloud service provider is responsible for the infrastructure security but the remainder is left to the consumer. PaaS security resides with the consumer and Cloud service provider. Each service model has a different risk level. Only security as it relates to PaaS and IaaS will be discussed in this paper. According to the Cloud Security Alliance (CSA), regardless of Service Model utilized in a Cloud environment, "Virtualization brings with it all the security concerns of the guest operating system, along with new virtualization-specific threats." (Cloud Security Alliance, 2011, p 157).

2.2. Information Security Standards and Guidelines

At the heart of any information security system is the requirement to protect the confidentiality, integrity and availability of data. There are numerous security standards that have evolved over the past several years. It is important to thoroughly understand your organization's security policies in order to implement like standards in a Cloud environment that will form your security frame work. Standards can be based on security, system development, financial reporting, IT service delivery, or control environment. Consequently, it is important to select a CSP who offers a standard that is most relevant to your business needs. By becoming ISO 27001 certified in May, 2012, Google Apps for Business reinforces to their customers that "…Google is committed to ongoing development and maintenance of a robust Information Security Management System (ISMS) that an independent, third-party auditor will regularly audit and certify." (Feigenbaum, E., 2012). Google has focused on information security whereas other CSPs may focus on health care (HIPAA) or financial (Sarbanes-Oxley). While the numbers of standards are numerous, I have focused on the most popular standards related to security.

The International Standards Organization (ISO) has published ISO/IEC 27001, an audit standard for Information Security Management Systems. Standards published by ISO intend to offer best practice but they are considered to be a measure of excellence in Information Security Management (Glass, 2009). The National Institute of Standards and Technology (NIST) publish a series of papers related to information security. The Federal Information Security Management Act (FISMA) of 2002 required the Federal Government to create standards for minimum information security and standards for categorizing information and information systems (FIBS Pub 200). The European Network and Information Security Agency (ENISA) is an agency of the European Union. The objective of ENISA is to improve network and information security in the European

Union. Other entities that create standards are Institute of Electronics and Electrical Engineers (IEEE), American National Standards Institute (ANSI) and National Security Agency (NSA).

While ISO 27001 and NIST standards outline a comprehensive security framework, the Federal Risk and Authorization Management Program (FedRAMP) was developed specifically for government agencies to assess and authorize cloud deployments with US government agencies. FedRAMP requirements are FISMA compliant and based on control areas in NIST 800-53, *Information Security.*

The range and depth of Information Security standards can be overwhelming. Fortunately, the Cloud Security Alliance has created a Cloud Controls Matrix (CCM). The CCM is designed to provide fundamental security principles to assist cloud customers in assessing the overall security risk of a cloud provider (CSA, 2012). Amongst others, the CCM consists of 13 domains based on ISO 270001 and NIST. The CCM creates an objective structure organizations can use to help satisfy compliance concerns and measure risks. Whether a CSP adheres to ISO, NIST, ENISA or FISMA standards, certification provides customers a sense of assurance that information security is a priority and a process to protect the confidentiality, integrity and availability of data is in place.

3. Security in the Cloud

3.1. Assessing Risk in the Cloud

Security in the world of information technology has become a popular topic within the industry and within the media. It is not uncommon to read about successful hacker exploits against consumers, business or government. As witnessed by the July, 2012 Dropbox security breach (Strauss, 2012) or the 6 million passwords that were stolen from eHarmony and LinkedIn, risks associated with Cloud computing are not necessarily reduced. The standard definition of risk by the ISO is, "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (Katsikas, 2009). The increased attack surface in a in a Cloud environment allows for other vulnerabilities to be exploited, thereby increasing the organization's risk. Virtual switches and the hypervisor are two examples of points of attack that are not present in the traditional data center. The attack surface can be defined as our exposure. Exposures are the vulnerabilities that are exploitable by the attacker (Northcutt, 2012). Consequently, an increased attack surface may increase security risks of Cloud security providers if the risks are not properly managed. According to a Gartner researcher Neil

McDonald, "through 2012, 60% or virtualized servers will be less secure than the physical servers they replace, dropping to 30% by YE 15." (McDonald, 2010, p. 2) Conversely, there are opportunities to reduce the security risks.

Risks can be decreased for small and medium sized business because there may be a lack of staff with specialization in information security whereas Cloud Service Providers (CSP) will have specialized staff that focus on information security. Because of economies of scale, it is cheaper to utilize a CSP than to design a high availability data center. The capability to provide a resilient, elastic and highly available computing platform is more cost effective for a CSP. In 2008 Oracle promoted their Oracle Database Backup to the Cloud service. Oracle promoted continuous accessibility, faster restores, better reliability and reduced tape backup and offsite storage cost. Many CSP meet compliance standards for information security (ISO 270001), healthcare (HIPPA), or finance (PCI). Such compliance certifications offer consumers a sense of confidence and trust in the CSP that a sound information security management system is in place. Risks that small and medium sized businesses are exposed may now be transferred to the CSP.

However, all risks are not mitigated by moving operations to a cloud environment. While some risks are reduced, other risks may increase. With the addition of virtual network switches, hypervisors and virtual images, the attack surface increases. According to NIST 800-133, cloud service offerings are complicated because resources are shared and unknown to the consumer (NIST, 2011). A single host with multiple virtual machines may be attacked by one of the guest operating systems. Or, a guest operating system may be used to attack other guest operating systems. Specific risks and means to mitigate those risks to the hypervisor and guest operating systems will be discussed later in the paper. Since cloud services are reached from the Internet, there is a possibility of wide spread disruption of service because of Denial of Service attacks or a more likely scenario of wide spread infrastructure failure (McMillan, 2012).

3.2. Traditional Security Overview

The methods to ensure information security that apply to the traditional data center consisting of racks of physical servers also apply to the virtual world. Platt defines three categories of information security: 1) Logical security, 2) Physical security, and 3) Premises security (Platt, 2009). Physical security protects the infrastructure, building and physical access to the data center. Premise security protects the people and property within the data center. It is important to ensure adequate physical security in is in place

and employees who may have access to your data are properly vetted. Logical security protects data using software safeguards such as password access, authentication, and authorization. Enforcing authentication and authorization help ensure the proper allocation of privileges (Tiller, 2007). Physical and premises security are under the direct control of the CSP but it is incumbent upon the customer to ensure strong logical security controls are maintained.

Physical, premises and logical security are part of a layered defense strategies where multiple layers of protection are employed reduce the risk of a successful attack. Even though one layer of protection may be compromised there are other layers that must be circumvented for the attacker to succeed. Traditional physical technical controls such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or Network Access Control (NAC) products that ensure access control continue to be critical components of the security architecture. However, these appliances no longer need to be a physical piece of hardware. A virtual firewall, for example, performs the same functionality as a physical firewall but has been virtualized to work with the hypervisor. Cisco, for example, provides a virtual firewall and security gateway that secures host computers containing virtual machines. (Cisco, 2012). According to Gartner analyst, Neil MacDonald, 40% of security controls in the data centers will be virtualized by 2015 (Messmer, 2012).

4. Applicability of Existing Security Tools

Traditional security tools such as firewalls or IDS/IPS can be virtualized to enforce security policies. However, conventional security controls designed for traditional hardware do not always map well to the cloud environment (VMware White Paper, p 6). While there are opportunities to improve security in the Cloud by using the same tools, there are still challenges to protect the virtual Cloud environment. I will address three features in a virtual Cloud environment that add to ensuring a secure security posture and methods to mitigate risks. Multi-tenancy, virtual networks and hypervisors add to the complexity.

4.1. Multi-tenancy

Arora, Biyani and Dave define multi-tenancy as pooled hosting environments in which more than one organization's applications and data are hosted on the same infrastructure, for example, within the same server (Arora, Biyani and Dave 2012, p100). Prior to the virtual world, these machines would be physically separated from each other.

In a Cloud data center it is the multi-tenant environment that allows economies of scale because a large number of virtual machines can be hosted on a single server. One of the risks in a multi-tenant environment is over provisioning of resources. Over provisioning resources results in resource contention and potential lack of availability, effectively creating a denial of service situation. Applications that are sensitive to latency, disk I/O or CPU utilization may be adversely impacted when there is resource contention. Performance may become unpredictable when "noisy neighbors" are co-located and start behaving poorly by consuming large amounts of CPU or memory resources. Ottenheimer and Wallace (Ottenheimer and Wallace, 2012) propose three mechanisms to reduce resource contention and move away from "noisy neighbors":

1) Re-provision VMs in hopes the VM will be provisioned on a host with adequate resources.

2) Crowd out other tenants by over provisioning.

3) Utilize fully reserved capacity.

As with physical servers, there are monitoring tools to help identify the source of contention. Resource availability should also be part of the Service Level Agreement that you have with the CSP.

Over provisioning or VM sprawl may be an unintended consequence of multi-tenancy. On the other hand, overt malicious attacks in a multi-tenant environment threaten the confidentiality, integrity and availability triad. As the number of guest VMs increase, the attack surface increases resulting in a greater possibility of successful malicious attacks on the virtual environment. A CSA recommendation is that implementers should ensure adequate security zones for different types of machines. Servers, development machines, workstations and management consoles should each have their own security zone (CSA, 2011, p 160).

In the last few years vendors have developed converged services that combine virtualization, networking and storage. For example, Cisco, VMware and Netapp have jointly designed a "best in breed Enhanced Secure Multi-Tenancy architecture. (Cisco, 2011). Integrating these three facets that are critical to deploying Cloud services provide a means to build a secure multi-tenant environment.

4.2. HYPER VISOR SECURITY

IBM published a paper in 2010 identifying six attacks against virtualized platforms (Williams, B. and Cross, T., 2010). They broke system virtualization vulnerabilities into six classes:

Management console vulnerabilities

Management server vulnerabilities

Administrative VM vulnerabilities

VM vulnerabilities

Hypervisor vulnerabilities

Hypervisor escape vulnerabilities

Hypervisor escape vulnerabilities are especially dangerous because other virtual machines residing on the host or the hypervisor may be exposed. As proof that hypervisor vulnerability is here to stay one only need to read the June 12, 2012 US – CERT bulletin regarding privilege escalation vulnerabilities on 64 bit processors running virtualization software (US-CERT, 2012). Because attacks against the hypervisor are rooted in the processor, traditional defenses such as firewalls and IPSs are not capable to stop them. Creating a chain of trust in the CPU that will extend to the hypervisor and hardening the hypervisor by following the manufacture's best practices are the best course of action to mitigate risks. Chain of trust is one mechanism to mitigate hypervisor risks. Mitre has published a detailed analysis of hypervisor vulnerabilities and mitigation. (McNevin, J., Schmeichel, R. and Faatz, D., 2010).

Liston and Skoudis describe several techniques to distinguish a physical machine from a virtual machine (Liston and Skoudis, 2006). Once a virtual machine is detected, the attacker can craft specific exploits against the VM and hypervisor. Research by IBM and the Department of Compute Science and Engineering, UCSD succinctly summarized hypervisor risks, "Although virtual machines are often marketed as the ultimate security isolation tool, it has been shown that many existing hypervisors contain vulnerabilities that can be exploited to escape from a guest machine to the host. We assume these attacks are somewhat likely" (Kurmas, Gupta, Plekta, Cachin & Haas).

4.3. ISOLATION OF NETWORKS

One of the critical responsibilities of the CSP is to provide a secure infrastructure that ensures customer's virtual machines are isolated in a multi-tenant environment and the various networks within the infrastructure are isolated from each other. Best practices suggest that the management networks, storage networks, and customer networks are all isolated. Isolation can be achieved by using virtual switches for each of the networks, utilizing 802.1q VLANs or a combination of both.

In a physical network Virtual Local Area Network (VLAN) is a method commonly used to isolate network traffic by creating a logical broadcast domain. Packets are tagged with VLAN identifiers that uniquely identify the VLAN number. Switch ports can be configured to accept specific VLAN traffic, thereby creating a logical layer of security. The principle of logically isolating network traffic between guest VMs becomes more important in a Cloud environment where a single host can support dozens of guest virtual machines. In order to maintain a multi-tenant environment, it is imperative that guest operating systems do not have the capability to communicate with each other unless designed to do so. As in the environment of physical servers, VLANs are an import component in the virtual world to ensure a secure multi-tenant environment. Separation at layer 2 or the data link layer of the OSI model is important to isolate virtual machine and management traffic from each other.

In the physical world each network interface card (pNIC) has a direct connection to a port on a physical switch. In the virtual world the physical NICs are connected to a virtual network switch via uplink connections. Port groups on the virtual switch are created with virtual switch ports and a corresponding VLAN id that enables VMs to access other VMs or the physical network. As depicted in Figure 2, this combination of a

virtual network that connects to the physical network ensures isolation of network traffic.

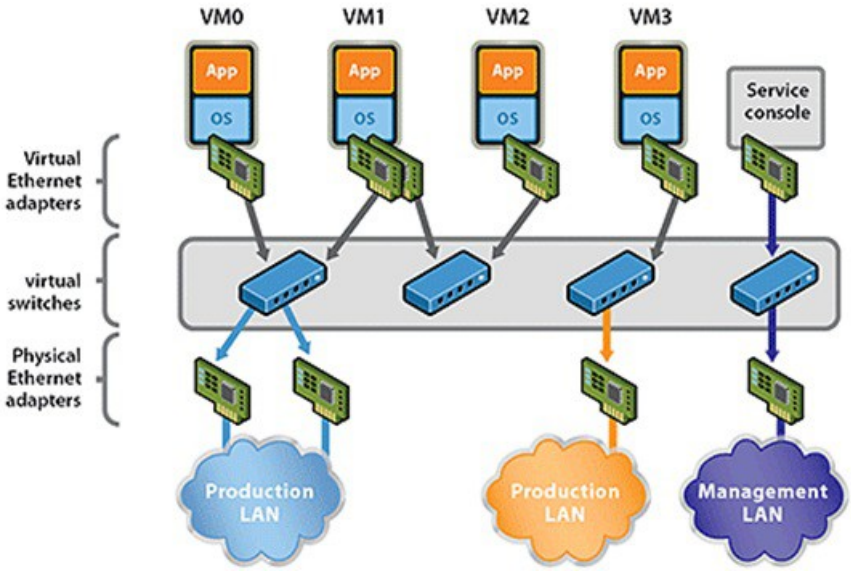

Figure 2

The management LAN is physically segregated using a physical NIC and its own virtual switch. Since access to the management LAN is akin to obtaining the "keys to the kingdom", it is imperative that Cloud administrators ensure the management LAN is adequately isolated from other guest operating systems. An additional layer of physical security would be to place the management LAN on it's a dedicated host with a virtual firewall separating it from other virtual machines, thereby effectively creating a logical DMZ or a logical security domain.

One of the benefits of using virtual machines in the Cloud is the ability to have duplicate virtual machines available on different hosts for disaster recovery purposes. If one host fails or maintenance needs to be performed on the host, the virtual machine can be moved to other host. The security risk is the movement from one host to another is not logged and often times the image is move while unencrypted. Anyone sniffing the network has an opportunity to extract critical information such as passwords or logins.

Traffic crossing the VM backplane is invisible to the traditional network tools mentioned above. (CSA, 2011, p 161).

4.3.1. Virtual Machine Introspection

One of the physical tools that does not map well to the virtual world are IDS and IPS scanners. A new architecture that utilizes virtual machine monitor technology allows better visibility into the monitored host. Researchers at Stanford University (Garfinkel T. and Rosenblum M.) wrote a paper describing how a virtual machine monitor can be used to inspect software on the inside. Virtual machine introspection (VMI) retains the characteristics of a Host Based Intrusion Detection System (HIDS) but allows better visibility into the virtual machine because of its access to the states of all the virtual machines. In addition, the Garfinkel and Rosenblum argue the VMM is difficult for an attacker to compromise and protecting the VMM is simpler than that of a traditional operating system. Consequently, the ability of a virus or rootkit to elude detection becomes more difficult. Commercial firewall products now include VMI as part of their products that are hypervisor based. According to an on-line article in Security Week, Johnnie Konstantas summarized VMI as "an agent-less way to peer into VMs and ascertain everything from their physical location (e.g., ESX host) to their network settings (e.g., VLAN assignment, IP and MAC addresses) right down to the installed OSes, patches, applications, and services—typically with negligible performance impact to the physical VM host." (Konstantas, 2010).

5. Protecting Data in the Cloud

Moving data to a Cloud environment presents an opportunity to achieve tremendous cost savings compared to the cost to purchase an equivalent amount of data for a locally hosted data center. As with virtual machines, a customer's data is stored over a shared infrastructure that may be distributed throughout multiple Cloud data centers. Adequate security measures must be in place to ensure unauthorized users cannot access data either intentionally or accidently.

5.1. Physical Security

The CSP must provide adequate infrastructure physical security to protect access to data. A combination of physical, administrative and operation controls should be in place to provide data security. Adequate protection of the CSP's facility by physical means such as guards, electronic badges and locks, biometric locks, and fences are important. Environmental safeguards such as fire detection and suppression, redundant

power supplies and climate control systems are also crucial. Geographic diversity is also crucial to maintain availability of data. Amazon and Google, for example, build their data centers in clusters in different global regions. Amazon utilizes N+1 redundancy as form of resilience that ensures system availability in the event of component failure (Amazon, 2011). It is incumbent upon the customer to ensure the CSP provides a secure environment with high availability.

5.2. Encrypting Data at Rest

Encrypting critical data 'at rest" will protect data confidentiality in the event the data is compromised. However, an assessment of your data must be conducted to determine what data needs to be encrypted. The SANS Institute states, "Encryption is most practical for data classification levels that are covered by regulatory or compliance mandates, as well as any sensitive internal data that needs to be protected at all costs." (SANS, 2012, p. 120). Encrypted data may be a file, a disk or an entire virtual machine. Encryption may be more challenging in the Cloud because data may be spread over several geographic locations and data is not on storage device dedicated solely to an individual business.

Sensitive or confidential information contained in files or folders can be encrypted before storing it to the cloud using traditional encryption tools such as GnuPG (free implementation of PGP) or the commercial version of PGP. The disadvantage to this is the additional steps to encrypt transmit the file and then decrypt it when the file is required. This can be a cumbersome procedure when working with files. A better approach is to use encryption that is inherent to an operating system. For example, Windows Encrypting File System (EFS) can be used to handle encryption and decryption of files and folders and make the process transparent to the user (Microsoft TechNet). The disadvantage to EFS is that it does not perform full disk encryption or full virtual machine encryption. However, full disk encryption (FDE) can be encrypted using a variety of encryption tools. Amazon's Linux systems can mount Elastic Block Store (EBS) volumes using encrypted file systems using EnFS, Loop-AES, dmcrypt or TrueCrypt. Lastly, an entire VM may be encrypted. High Cloud Security offers a product that performs encryption on the entire VM. High Cloud Security provides for secure virtual machines, key and policy management, VM optimized storage to ensure encryption and auditing and reporting.

While encryption to protect data at rest seems obvious and simple, there are challenges to consider. Anytime a file or disk is encrypted additional processing time is

required. Even though encrypting or decrypting a file or performing a FDE may not consume a large amount of additional resources, the sum of the requirements required to perform these actions may adversely impact performance in a multi-tenant environment with a pre-defined amount of pooled resources. Secondly, encryption of data at rest used in a cloud application will prevent indexing or searching of that data (Mather, Kumaraswamy & Latif, 2009). Thirdly, key management may become an issue. If the key is lost, the data is lost. If the key is compromised, then the data may be compromised. Consequently, key management is an important factor when entering into an agreement with a CSP.

5.3. Encrypting Data in Motion

Data in motion to and from the CSP is no different than data in motion when using the Internet for other business needs when data in transit needs to remain confidential. However, it is incumbent upon the consumer to ensure data within the CSP infrastructure moves within and between their data centers in a secure manner. SSL/TLS is used to securely move traffic across the Internet.

Traditionally, data is either encrypted while it is at rest or in motion. In a June 2009, eWeek.com on-line article, Brian Prince reported that IBM had discovered an encryption that allows data to be processed without being decrypted (Prince, 2009). The researchers developed a fully homomorphic encryption scheme. Homomorphic encryption is the conversion of data into ciphertext that can be analyzed and worked with as if it were in plaintext form. This has direct implications to storing data in the Cloud because data stored in an encrypted state in the Cloud can be searched, indexed or manipulated while remaining in an encrypted state. Currently, the data has to be decrypted off the Cloud or the Cloud requires access to the data. As confidence in data remaining confidential while remaining in the Cloud will entice businesses to move data to the Cloud.

6. Monitoring and Incident Response

The ability to monitor logs change when computing resources are moved to a Cloud environment. Since incident response relies heavily on log data for detection and forensics, an organization's incident response plan will need to be modified.

6.1. Monitoring

One of the potential draw backs of moving data processing to a Cloud environment is losing direct control. Administrators who previously had direct access to physical servers and console access now have limited accessibility. However, according to NIST Publication 800-53, “Organizations are accountable for the risk incurred by use of services provided by external providers and address this risk by implementing compensating controls…” (NIST, 2009, p.12). The challenge has become to work with the vendor to ensure adequate monitoring tools are in place to capture logs from operating systems, applications and hardware devices. These logs often contain crucial information if a system is compromised. A recent survey conducted by Jerry Shenk, a Senior Analyst for the SANS Institute, revealed that 82% of the respondents used logs to track suspicious behavior. From a security perspective, access to log information is important to being proactive in detecting malicious activity.

Unfortunately, depending upon the service offering (i.e. Iaas, PaaS, SaaS) only some of the necessary logs will be available. Obtaining IaaS logs are the most easily obtained? Security, application, or system logs from a Windows server and syslog output from a Linux server can be captured as if the servers were housed locally. PaaS and SaaS log retrieval may be more difficult according to Gartner analyst Anton Chuvakin, "When organizations move to public cloud computing, the role of application logging will increase, since in SaaS and PaaS environments familiar OS logs simply don't exist. Sadly, organizations today are having trouble analyzing application logs from traditional on-premises applications, even without the whole cloud aspect blended in." (Schackleford, 2012, p. 2). The issue is further complicated by the fact that logs are aggregated in a multi-tenant environment and not shared by the CSP. In contrast to a traditional data center where the administrator has direct access to Windows, Linux, or syslogs, logs gathered in a Cloud environment may be a combination of various different customers combined into one log. In an article about SLAs by Buck and Hanf, SLAs need to detail the exact logs available (Buck and Hanf, 2010).

Monitoring at the OS or VM level is a basic means to monitor your systems but to closely monitor attacks tools such as an Intrusion Detection System (IDS) can be used. There are more considerations when implementing virtual IDS in a virtual environment. For example, because of an internal virtual network, it is more difficult to place a traditional IDS appliance in-line into a virtual environment. Host based IDS will function in a virtual world but an agent based host IDS will consume resources from the resource

pool. If there are numerous host based IDS (HIDS) installed, then performance will be affected.

While the design to implement virtual IDS may be more challenging, it is possible to continue to use traditional security tools. According to SANS, there are three methods to allow intrusion detection monitoring in a virtual environment (SANS, 2012):

> Enable promiscuous mode on a Port Group or vSwitch. A virtual IDS will be able to monitor traffic on the virtual network segment.
>
> In an IaaS environment, install a virtual appliance in-line.
>
> Utilize SPAN technology mirror a port to capture traffic.

A CSP may offer the customer the capability to monitor for malicious traffic by using and IDS. VMware expert Dave Schackleford, outlines several factors to be aware of if you implement your own IDS in an IaaS environment:

1) Make sure you can adequately monitor network traffic using "virtual taps" or port mirroring.
2) When using HIDS, be wary of resource consumption.
3) Consider how the IDS will be monitored. It may be necessary to connect monitoring consoles to the Cloud via a VPN connection.

6.2. Incident Response

The nature of incident response will be impacted when services are moved to the Cloud. According to the Cloud Security Alliance, the customer must consider what must be done to enable efficient and effective handling of security incidents in the Cloud (CSA, 2011, p. 93). Given the possibility that log information may be directly inaccessible to the customer, the incident response team will need to take into consideration the type of service being utilized (i.e. IaaS, PaaS, SaaS) and craft a security SLA to address responsibilities of the CSP. For example, if SaaS is being utilized, then the CSP incident response team will internally respond to triggers from their Security Incident and Event Manager (SIEM), IPS/IDS tools or other log management tools. In this scenario, the customer has no responsibility. However, it is important to include a notification process in the SLA, especially if personal information is at risk. If PaaS is being utilized, then the incident response team will have access to application logs but the CSP will still maintain server logs. The customer has more opportunity to retrieve log

information from a PaaS provider by communicating to the CSP what triggers an event (SANS, 2012). Examples of triggers can be failed authentication attempts or application errors. If the service provided is IaaS, then the CSP is responsible for the infra-structure related logs such as storage, networks and hypervisors. The customer will have access to their VM logs and IDS logs during an incident.

Services such as SaaS or PaaS may make incident response easier because the burden rests upon the CSP. Incidents that require obtaining an image or snapshot of the virtual machine for forensics is also easier because a virtualized environment is designed to copy or clone images, including memory states. Special software is no longer needed when the inherent capability of your virtual platform provides these functions. Procedures of the incident response team will need to be modified to accommodate the new environment.

7. Conclusion

Business and government will continue to move a Cloud environment in an effort to reduce costs, improve efficiencies and reduce administrative overhead. Delivering IT services via the Cloud portends to be a time saver, a money saver and allow for better efficiencies. This new paradigm of computing offers many benefits but it also increases security risks.

The delivery of computing resources in a Cloud environment is elastic, available on demand and convenient for the customer. While not mandatory, virtualization of the data center is important to achieve economies of scale that enable services to be provided at a lower cost than a traditional data center. While virtualization reduces some security risks, others are increased because the attack surface in a Cloud service increases. Traditional security methods are still relevant in the Cloud but are implemented in a virtual means. In a virtualized Cloud environment customers are segregated into separate security zones called multi-tenancy. Virtual NICs, virtual switches and port groups add complexity but allow a multi-tenant environment.

Data is protected by traditional means such as physical security, encrypting the data at rest and data in motion. Data in motion is still sent across the wire using SSL but encrypting data in the Cloud's virtual data center presents challenges. Cloud Service Providers cannot process encrypted data in the virtual data center so the data must be encrypted locally then transmitted. However, homomorphic encryption may be a solution to the encryption challenge but is not likely to be a feasible solution for several years.

Todd Steiner, tsteiner@innd.uscourts.gov

Customers must work closely with their service provider to ensure adequate logging and monitoring is available. Incident response plans will also need to be modified to meet the changes. When entering into an agreement with a service provider it is important to ensure requirements for monitoring, logging, encryption and security is part of a Service Level Agreement.

Todd Steiner, tsteiner@innd.uscourts.gov

8. References

Amazon. (2011). *Amazon Web Services: Overview of Security Processes.* Retrieved from http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

Arora, P., Biyani, R. and Dave, S. (2011). *To the cloud: Cloud powering an enterprise. McGraw-Hill.*

Buck, K. and Hanf, D. (2009). *Mitre cloud computing series, Cloud SLA considerations for the government consumer.* Retrieved from http://www.mitre.org/work/tech_papers/2010/10_2902/cloud_sla_considerations_government.pdf

CBS News Staff. (2012, June 7). CBS News. Retrieved from: http://www.cbsnews.com/8301-501465_162-57448965-501465/eharmony-suffers-password-breach-on-heels-of-linkedin/

Cisco. (2012). *Cisco asa 1000V cloud firewall data sheet.* Retrieved from http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps12233/data_sheet_c78-687960.pdf

Cisco. (2011, July 7). *Deploying enhanced secure multi-tenancy into virtualized data centers.* Retrieved from http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/securecldeployg_V2.pdf

Cloud Security Alliance. (CSA, 2011). *Security guidelines for critical areas of focus in cloud computing, v3.0.* Retrieved from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Cloud Security Alliance. (CSA, 2012). *Cloud Control Matrix*, Retrieved from https://cloudsecurityalliance.org/research/ccm

Coleman, C. (2012, September 25). *Cloud conversion saves gsa millions*. Retrieved from http://gsablogs.gsa.gov/gsablog/2012/09/25/cloud-conversion-saves-gsa-millions/

Feigenbaum, E. (2012, May 28). *Google Apps receive 27001 certification.* Google Enterprise Blog. Retrieved from

http://googleenterprise.blogspot.com/2012/05/google-apps-receives-iso-27001.html

Glass, D. (2009). Security audits, standards, and inspections. In S. Bosworth, M. Kabay & E. Whyne (Eds.), *Computer Security Handbook* (Vol. 2). Hoboken, New Jersey: John Wiley & Sons, Inc.

Jansen, J. National Institute of Standards and Technology, (2011). *Guidelines on security and privacy in public cloud computing*. Retrieved http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494

Katiskas, S. (2009). Risk management. In J. Vacca (Ed.), *Computer and information security handbook.* Bedford, MA: Morgan Kaufmann Publishers.

Konstantas, J. (2010). Vm introspection. know your virtual environment inside and out. *Security week*, Retrieved from http://www.securityweek.com/vm-introspection-know-your-virtual-environment-inside-and-out

Kumar, S. (2008). *Oracle database backup in the cloud, An Oracle white paper.* Oracle Corporation. Retrieved from http://www.chinacloud.cn/upload/2010-02/10021216486604.pdf

Kurmas, A., Gupta, M., Plekta, R., Cachin, C., & Haas, R. (n.d.). *A comparison of secure multi-tenancy architectures for filesystem storage clouds*. Informally published manuscript, IBM Research and Department of Computer Science and Engineering, UCSD. Retrieved from http://www.zurich.ibm.com/~cca/papers/scs.pdf

Liston, T., and Skoudis, E. (2006). *On the cutting edge: Thwarting virtual machine detection.* Retrieved from http://handlers.sans.org/tliston/ThwartingVMDetection_Liston_Skoudis.pdf

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy*. Sebastopol, CA: O'Reilly Media.

McDonald, M. (2011). *Reimaging it: 2011 cio agenda,* Gartner Executive Programs. Retrieved from

http://www.gartner.com/resources/210300/210382/executive_summary_reimagin_210382.pdf

McDonald, N (2010). Gartner Research. *Addressing the most common security risks in data center virtualization projects.* Retrieved from http://bsius.com/media/182447/addressing_the_most_common_s_173434.pdf

McNevin, T., Schmeichel, R., and Fattz, D. (2010). *Mitigating hypervisor vulnerabilities.* Retrieved from www.mitre.org

Messmer, E. (2012, June 12). Gartner: Network virtualization will lead to security control changes. *Network World,* Retrieved from http://www.networkworld.com/news/2012/061212-gartner-macdonald-260107.html

McMillan, R (2012, October 12). Amazon cloud goes down again, breaks foursquare and others. *Wired,* Retrieved from http://www.wired.com/wiredenterprise/2012/10/amazon-web-services

Mell, P and Grance T. National Institute of Standards and Technology (NIST). (2011). *A definition of cloud computing*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Microsoft TechNet. (2012). Microsoft TechNet, *The encrypting file system*, Retrieved from http://technet.microsoft.com/en-us/library/cc700811.aspx#XSLTsection126121120120

Northcutt, S. (2011). *The attack surface problem,* Retrieved from: http://www.sans.edu/research/security-laboratory/article/did-attack-surface

Ottenheimer, D., & Wallace, M. (2012). *Securing the virtual environment*. Indianapolis, IN: John Wiley and Sons.

Prince, B. (209, June 25). Ibm discovers encryption scheme that could improve cloud security, spam filtering. *eWeek.com,* Retrieved from http://www.eweek.com/c/a/Security/IBM-Uncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering-135413/

SANS (2012), Cloud Security Fundamentals, Security 524, Volume 2, *Cloud Security.* The SANS Institute.

Schackleford, D. (2012, November). Logging in the cloud: Assessing the options and key considerations. SearchCloudSecurity.com Retrieved from http://searchcloudsecurity.techtarget.com/tip/Logging-in-the-cloud-Assessing-the-options-and-key-considerations

Schackleford, D. (2012, August). Intrusion detection in the cloud: Public cloud ids considerations Retrieved from http://searchcloudsecurity.techtarget.com/tip/Intrusion-detection-in-the-cloud-Public-cloud-IDS-considerations

Shenk, J. (2012). Sorting thru the noise, SANS eighth annual 2012 log and event management survey results. Retrieved from http://www.sans.org/reading_room/analysts_program/SortingThruNoise.pdf

Strauss, K. (2012, July 19). Dropbox security breach: Who's guarding your secrets in the cloud. *Forbes.* Retrieved from http://www.forbes.com/sites/karstenstrauss/2012/07/19/dropbox-security-breach-security-in-the-cloud/

Tiller, J. (2007). Access control. In H. Tipton & K. Henry (Eds.), *Official (ISC)2 Guide to the CISSP.* Boca Raton, FL: Auerbach Publications.

US-CERT (2012), Sysret 64-bit operating system privilege escalation vulnerability on intel cpu hardware. Retrieved from: http://www.kb.cert.org/vuls/id/649219

Wilcox, J. (2011). *Gartner: Most cios have their head in the cloud*. Retrieved from http://betanews.com/2011/01/24/gartner-most-cios-have-their-heads-in-the-clouds/

Williams, B and Cross, T, (2010), IBM Internet Security Systems, *Virtualization system security.* Retrieved from http://blogs.iss.net/archive/papers/VirtualizationSecurity.pdf

Todd Steiner, tsteiner@innd.uscourts.gov

Last Updated: August 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Fall 2017	OnlineCAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced