Storm Clouds - Security Issues in the Cloud and How to Address Them

Author: Mike Pittenger

25+ years in operations, business development, marketing and sales. Most recently VP Sales and Marketing at Savant Protection, a provider of security software for application whitelisting.

VP & GM of @stake, acquired by Symantec in 2004. Ran the Product Division for award-winning security products: l0phtCrack (LC5) & SmartRisk Analyzer, Information Security's 2004 Product of the Year.

Founded Veracode; built upon SmartRisk Analyzer core technology - launched industry's first application risk management platform to automatically identify security vulnerabilities in application binaries.

Introduction

The cost-benefits of cloud infrastructure services include scalability with reduced capital expenditure and more efficient use of IT resources. Fully managed cloud infrastructure services and applications allow enterprises to focus on their core competencies rather than IT or application management. IDC estimates *cloud-based infrastructure software and application services* represent 79% of a total 2009 cloud services market of $17.4B, or approximately $14B.[1]

Enterprise IT security technology, policies and procedures need to be augmented rather than revolutionized to accommodate new attack surfaces that may be introduced by cloud computing. The most effective approach is still a layered defense, based on a security framework. The framework will encompass familiar domains: securing the operating platform; identity management and administrative access control; and protecting data at rest as well as in transmission. A strong cloud infrastructure defense must also leverage new tools at logical infrastructure layers and protect the integrity of communications via the Internet.

Additional Benefits of Cloud Infrastructure Services

Enterprises with limited IT resources may require fully managed IaaS and enterprise applications to realize cost benefits; mid-sized enterprises simply may not be able to afford to manage IT and remain competitive. Larger enterprises may leverage hybrid solutions, combinations of on- and off-premises private cloud or service provider virtual machines, to minimize IT spending, and gain the benefits of "elasticity," while reducing the time required for provisioning.

But both types of enterprises can benefit from the security experience and "economies of scale" provided by a cloud service provider. Because of scale (and business exigencies) the provider has more resources and is compelled to implement adequate security technology and procedures. Because of the virtual infrastructure, specifically a logical software layer, the vendor can implement standards-based, uniform security measures more rapidly than in the physical world. *In many cases, the cloud vendor may provide better security in a virtualized environment than the individual enterprise can achieve in a purely physical architecture.*[2]

Evolution of Cloud Infrastructure Services

Initial IaaS[3] benefits were derived largely from virtualization technologies. Virtualization is the partitioning of computer processing and memory into distinct, isolated instances running on the same physical machine. Virtualization also provides a consolidated, logical view of multiple virtual machines – through a hypervisor. Virtualization allows for more efficient use of servers (including all the datacenter and support costs), and independence from specific machine limitations.

Automation tools within the datacenters and self-service provisioning of virtual machines via Web portals delivered increasing agility (speed) and flexibility responding to changing enterprise IT requirements. The cloud-based IaaS model continues to evolve.

[1] Total cloud spend on "Application Software, Application Development and Deployment Software, Systems Infrastructure Software, and Server and Disk Storage capacity. These figures do not include spending for private cloud deployments; they look only at public IT cloud services offerings." See "Worldwide IT Cloud Services Revenue by Product/Service Type", IDC, September 2009.

[2] See "Security Compliance in a Virtual World: Best Practices to Build a Solid Foundation", RSA Security Brief, 2009.

[3] See Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, pg 19: "IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources (or not), as well as deliver physical and logical connectivity to those resources. Ultimately, IaaS provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers."

Cloud IaaS is becoming more responsive to *business drivers originating beyond IT*. Cloud infrastructure services now encompass line-of-business requirements, such as customer relationship management, e-commerce, and enterprise financials.[4]

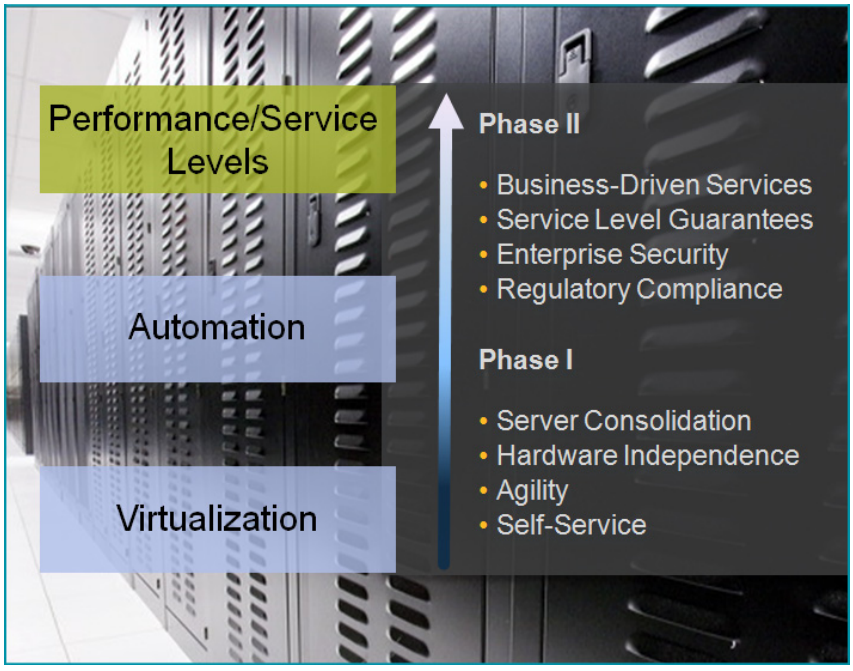
Embracing outsourcing, the enterprise is looking for broader service level guarantees, and for help integrating cloud IaaS and applications into existing compliance regimens, such as Sarbanes-Oxley (SOX), Gramm Leach Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accounting Act (HIPAA).

Security Frameworks, the Regulatory Environment and IT

IT is being called upon to play a greater role in meeting ever more compliance requirements. Compliance legislation for different business types and departments within the enterprise will influence, and in some cases dictate security requirements – examples include GLBA and SOX reporting for publicly held companies; PCI DSS and HIPAA for those dealing with cardholder data and medical records; and Personally Identifiable Information (PII).

And the compliance environment is only going to become more demanding and complex. The enterprise doing business across international borders, and even state lines, must contend with expanding PII legislation. For all segments, meeting compliance will require more resources – and not just in IT. The value of up-to-date, standards-based security provided by managed cloud infrastructure services will only increase.

Figure 1: Evolution of Cloud Infrastructure Services



Security Frameworks and Cloud Services

Security professionals recognize the better way to approach enterprise security is working within a holistic framework. Primary examples include the ISO information security standards 27000 series or the Control Objectives for Information and Related Technology (COBIT).[5] Though the cloud model does present unique security challenges -- for example protecting virtual environments -- the steps required to strengthen cloud infrastructure services are not foreign to existing frameworks.

Several industry organizations have begun addressing security in cloud deployments. The Cloud Security Alliance (CSA), working closely with IEEE and European Network and Information Security Agency (ENISA), recently published the "Top Threats to Cloud Computing V1.0". Within the European Union, ENISA has

[4] See "Who still keeps money under their mattress? The case for cloud security", Ryan Nichols, June 10 2010, http://blogs.computerworld.com .

[5] Published by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA). http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx .

published the "Cloud Computing Information Assurance Framework" and other supporting risk assessment documents.[6]

These resources can be used in conjunction with existing holistic frameworks to help focus on specific cloud deployment and business (compliance) requirements. The security technology and best practices described below for cloud infrastructure services and applications provide the building blocks for augmenting security frameworks.

Addressing Vulnerability Concerns in Cloud Infrastructure Services

Four areas of concern are critical when securing cloud infrastructure services and managed enterprise applications. In and of themselves these are not unique to the cloud – but addressing them may require new tools or a different approach.

Ultimately the enterprise is responsible for a security posture. The widely accepted characterization is a "trust but verify" relationship with the cloud service provider.[7] The enterprise must be proactive regarding SLAs, reporting, and defining security responsibilities – in effect taking on audit-like responsibilities, just as management should demand from an in-house IT organization. Deploying cloud infrastructure services represents an opportunity for the enterprise to leverage the greater resources available from the IaaS provider and build in security from the ground up.

Platform Hardening

Virtualization adds new layers to the infrastructure: the hypervisor (or virtual machine manager), and the administrative layer. Though virtualization, to a large degree, enables cloud benefits, the additional layers may also introduce new vulnerabilities. Virtual machines running on the same physical machines must be guaranteed not to 'bleed over,' whether through omission, mis-configuration, or intentional attacks.

The Center for Internet Security and the Defense Information Systems Agency (DISA), as well as hypervisor vendors of VMware and Citrix (XEN), publish 'hardening' guidelines that are "well-established and accepted as industry best practices."[8]

These guidelines define proper configurations, the deployment of the latest patches, and the secure removal of unused components, for example how to protect memory segmentation correctly using container rings. In a virtual environment, platform hardening also requires the *securing of deprovisioned virtual machines and resources* -- the adequate cleaning up of virtual machines when reallocated or decommissioned.

In aggregate, these steps provide layered defenses to guarantee virtual machine isolation as well as challenge penetration from outside. Properly hardened hypervisor layers prevent IaaS end-users from inadvertently mapping IP addresses across virtual machines, spoofing IP addresses, or intentionally leveraging Network Address Translation (NAT) to hijack communications. Hardening also makes it extremely difficult to install 'eavesdropping programs' to monitor the way virtual machines are using memory space.

'Intelligent' Layer 2 Switch

A layer 2 network switch deployed with the hypervisor affords an additional layer of defense. Configured correctly, an 'intelligent' switch can 'lock down' Media Access Control (MAC) addresses, and perform dynamic inspection of the Address Resolution Protocol (ARP) process. Used in conjunction with authentication protocols, they help mitigate man-in-the-middle attacks and ARP cache poisoning.

---

[6] See "Cloud Computing Risk Assessment", http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment .

[7] See "IBM Point of View: Security and Cloud Computing", pg 4, November, 2009.

[8] See "Security Compliance in a Virtual World", RSA Security Brief, August, 2009.

These same logical layers that provide a consolidated view of multiple virtual machines can help the security administrator rapidly propagate layered security policies across the infrastructure. This is an opportunity to be proactive rather than reactive. If properly managed, this level of abstraction can actually strengthen security, and make it easier to implement.

Identity Management and Administrative Access Control

As with any enterprise system, identity management is a key component of security. For clients accessing their accounts, multi-factor authentication is a baseline requirement. Best practices also include role-based access management. Role-based access control allows permissions to be mapped to specific business functions or support groups. Such a system instantiates written access policies, and provides an additional layer of user discrimination – and detection – in system access.

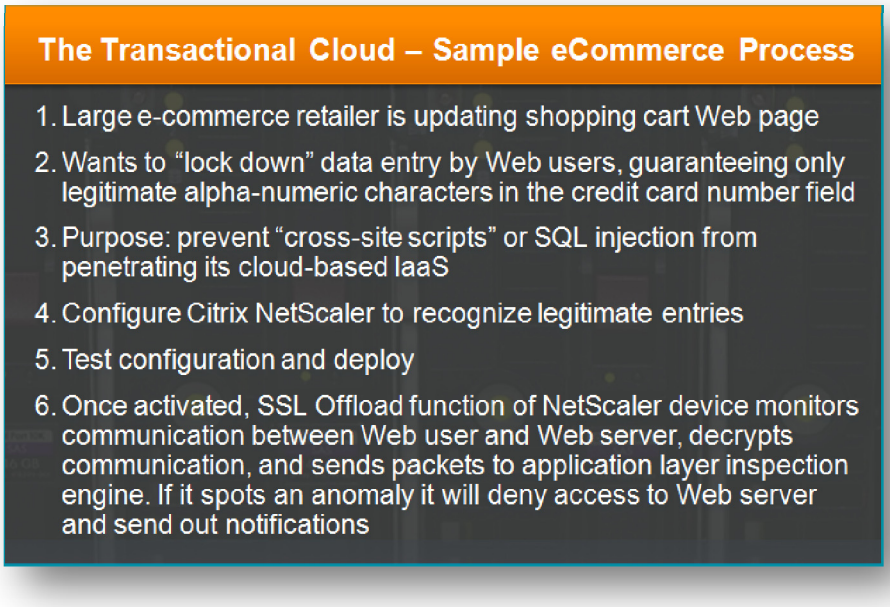
Administrative access control takes on increased urgency in the virtual environment. Inherent in the power and scope of the hypervisor is the potential for misuse or abuse by authorized users. Strict employee screening and qualification, which should be a part of any security policy, take on even greater significance. Segregation of duties is paramount. Administrative functions previously done through different consoles, such as server and network activation, may now be consolidated in the hypervisor. Each role should have defined granular privileges separate from another, and the principle of least privilege should be employed. It is important to manage the activities of privileged third parties; best practices are to have all third-party activity monitored by staff.[9] Because of the number of physical servers and likely geographic distribution, it is important to manage carefully, even disable local administrative functions.[10]

Privileged Identity Management

Best practices dictate frequently changed, unique passwords for privileged accounts. Given the scale of cloud infrastructures and the consolidation of administrative access via the hypervisor, it is worth considering Privileged Identity Management (PIM) software.

A fully supported PIM application can help enforce administrative access rules – greatly mitigating the risk of undocumented and/or malicious access to configuration settings and private data. PIM software can support IT best practices such as those promoted by Information Technology Infrastructure Library (ITIL), and provide audit trails required for compliance regulations SOX, GLBA, PCI-DSS and HIPAA. The more advanced packages can perform continuous discovery across new hardware and software applications, and can rapidly and comprehensively propagate changed

Figure 2: Leveraging the Transactional Cloud



[9] See "How to Secure Sensitive Data in Cloud Environments", Slavik Markovich, eWeek, April 21, 2010.

[10] See "Security Compliance in a Virtual World", RSA Security Brief, August, 2009.

passwords after third party access or staff turnover.[11]

Network Segmentation and Traffic Protection

As with virtual machines, the segregation and protection of data flowing through virtual or private LANs (VLANs or PVLANs) is paramount. This begins in the hypervisor hardening process with proper network configuration and permissions. The hypervisor and virtual administrative layer establish the secure Media Access Control (MAC) address assignments and restrict Network Address Translation (NAT).

Further inter-VLAN protection comes from the proper deployment and configuration of firewalls. A layered network defense may consist of multiple firewalls; a layer of physical firewalls and a layer of virtual or host-based firewalls; or a layer of firewalls combined with other access control methods. Firewalls, perhaps in addition to port forwarding schemes, should be in place between VLANs. In cloud IaaS environments, *an application-layer firewall should be placed monitoring any Web application traffic*. An application-layer firewall can be software or a dedicated appliance, and permits only defined application behavior. They also provide an additional layer of defense against distributed denial of service (DDoS) attacks.

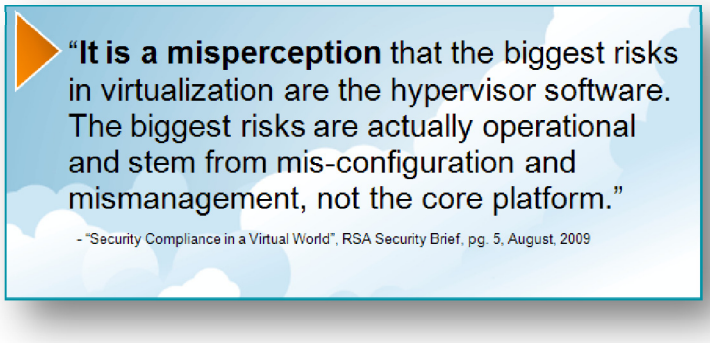
Encryption

Given different business and compliance requirements, it is the responsibility of the client to determine what data to encrypt and the strength of encryption. Guidelines however are clear. It is standard practice that, at a minimum, data in transit be protected with SSL configurations on virtual machines.

Administrative communications from clients, for example via a Web portal, should employ SSL VPN. Data at rest should also be encrypted, the strength and scope of which is determined by the security policy. For example, to meet PCI DSS compliance all cardholder PII must be encrypted. Encryption key management may also be part of a cloud infrastructure service.

Operational Security

It is well documented many security breaches result from mis-configured software or an out-of-date security posture. The significance of change management is heightened in a virtual environment – with a logical layer that can apply patches across multiple 'machines,' and the potential scope of mis-configuration. Best practices require change management be administered through the hypervisor layer, or a standards-based application leveraging the hypervisor functions.



The significance of change management is heightened in a virtual environment – with a logical layer that can apply patches across multiple 'machines,' and the potential scope of mis-configuration. Best practices require change management be administered through the hypervisor layer, or a standards-based application leveraging the hypervisor functions.

More and more compliance requirements include the ability to audit system changes – not just patches -- firewalls, privileged access, and in the virtual environment, provisioning and de-provisioning. Best practices require that systemic logging of any changes to firewalls, such as provisioning of machines, IP addresses, NAT mapping, and administrative access, be designed into the user interface.

[11] See "Privileged Identity Management in the Cloud", Steve Staso, pgs 19-20, April, 2010.

Logging system change data is not only for compliance purposes; it is imperative for the tracking of incidents, errors and process improvements. Maintaining a strong security posture has never been a static endeavor. The cloud service provider must continue to monitor and adjust. In the virtualized realm, the speed of attacks and scope of vulnerability due to error or omission can only be met by rapid detection and mitigation.

Figure 3: Addressing CSA's 'Top Threats to Cloud Computing v1.0'

CSA Top Threats	Suggested Remediation
Abuse and Nefarious Use of Cloud Computing	All customers are subject to a formal sales process prior to provisioning on the cloud allowing for much more control over user identity
Unsecure Interface and API	Access to the management console should be protected with strong authentication (two-factor); no customer API access should be allowed
Malicious Insiders	All Cloud Service Provider employees should be subject to background checks prior to employment; all activities executed through a cloud computing management interface should be recorded
Shared Technology Issues	The cloud platform hypervisor should be configured in accordance with VMware and industry best practices for hardening
Data Loss or Leakage	VMs should be securely deleted from the underlying disk when removed via the Web interface. Additional technologies such as Strong Encryption and PKI, should be added to individual VMs
Account or Service Hijacking	Employ strong authentication for the cloud management interface and make recommendations to cloud users to create dedicated accounts for each end user
Unknown Risk Profile	Provide customers with access to 3rd party audit reports attesting to adherence to security controls for the cloud and physical hosting platforms

A baseline technology is a Network Intrusion Detection System (IDS). Additional security is provided by a security information and event management (SIEM) console. A SIEM system allows logged events from the hypervisor, firewalls, the IDS system, and other components, to be monitored and correlated for a more complete picture. For example, a SIEM system can help track the provisioning of virtual machines or patterns of behavior by specific individuals over time.

Proactive Management

The strongest layer of defense is proactive system management. Proactive security management is best demonstrated in the experience of the cloud service provider. A proactive security posture includes a documented, standards-based incident escalation and notification procedure, regular automated vulnerability scans, file-integrity monitoring software, and investment in on-going system and security training.

The benefits of proactive security are even more evident in cloud infrastructure services and managed enterprise applications. If the cloud provider does not have experience fully managing cloud infrastructure as

opposed to simply provisioning, there is risk. Likewise, if the service provider does not have experience managing specific business applications (Oracle E-Business Suite, Siebel, Hyperion, etc.), there is also risk.

Future Trends

Technology is emerging that will further strengthen cloud computing. The "hardware root of trust" initiative is an effort to provide ultimate visibility and security throughout IaaS hardware, literally down to the chip level.

Employing secure computing chips, such as Intel's Trusted Execution Technology, the system scans hardware and software components at each step of the boot sequence. If the component profile matches 'trusted profiles,' stored in cryptoprocessors within the hardware, the "hardware root of trust" preserves a snapshot of the component and allows it to join the system.[12]

Encryption for use in cloud deployments is another area of development. Data encrypted with current algorithms are hard to search or perform calculations on, which means it must be stored in the cloud unencrypted, or 'pulled back' to secure servers where it must be decrypted to be useful. Given the scale of many cloud data sets and applications, for instance in banking and healthcare, this is simply impractical. But emerging encryption technologies allow for search, retrieval, and calculation all within the cloud. And other research is looking at hierarchical encryption schemes that would provide different levels of access to users.[13]

Summary

The cost-benefits of cloud infrastructure services and managed enterprise applications continue to drive more enterprises to cloud deployments. Fully managed cloud-based applications allow enterprises to focus on their core competencies – not application management. Mid-size and large enterprises can enjoy the elasticity of the cloud but leverage the application management investment and expertise of the service provider.

The most effective security is still a layered defense based on a framework. Security technology and procedures are augmenting existing security frameworks to accommodate cloud architectures. Managed cloud deployments offer the opportunity for the enterprise to build in security from the ground up. In fact, properly configured and managed, enterprise security in the cloud may be greater than what they could achieve on their own.

About NaviSite Managed Cloud Services (MCS)

NaviSite's Managed Cloud Services enable on-demand scalable provisioning of IT services including applications, servers, storage, and networks. The NaviCloud Platform offers unique enterprise IT advantages that tap into the core of NaviSite's application and enterprise infrastructure management expertise.

Designed specifically to meet enterprise IT demands, the NaviCloud Platform delivers services on best-of-breed technology infrastructure from leading vendors including Cisco Systems™ and VMware™ - all provided under one of the industry's strongest SLAs. Whether supporting seasonal computing demand spikes, creating robust and cost-effective software testing and development environments, or building full application lifecycle management for mission critical enterprise applications, the NaviCloud Platform offers today's premiere cost-effective enterprise-class infrastructure option.

To contact a NaviSite MCS security expert, please visit us at http://www.navisitemcs.com or call 877-485-9251.

[12] See "RSA Cloud Security Brief: Infrastructure Security: Getting to the Bottom of Compliance in the Cloud", March, 2010.

[13] See "Security in the Ether", David Talbot, MIT Technology Review, pg 41, Jan/Feb 2010.