Silver Linings: Securing your Data in the Cloud

Kaizen Approach Inc.

What is the Cloud ?

- Virtualized services
- Service is sold on demand
- Service is elastic -- a customer can have as much or as little of a service as they want at any given time
- Service is fully managed by the provider
- Different types of cloud models and services offered

Cloud Services

- Most Common Services:
  - SAAS – Software as a Service
    - Tenant owns the data used by the application but does not support any part of the infrastructure (GoogleApps)
  - IAAS – Infrastructure as a Service
    - Tenant has ownership of everything above the virtualization layer (Amazon Web Services EC2)
  - PAAS – Platform as a Service
    - Tenant has ownership of the applications and code; the provider manages the databases, web servers, and operating system (Windows Azure Compute)

Why use the Cloud ?

- Cost efficient – lower IT costs for personnel, space and equipment
- Faster deployment of applications
- Easier management of backups, recovery, software management (depending on what cloud service used)
- Accessible from anywhere there's Internet access
- Increased storage
- Flexibility to make changes to applications
- Enables small businesses without a significant IT staff to consume services it might not otherwise afford

Cloud Types

- Public – Shared by multiple customers
- Private – Accessed by one customer
- Community – Shared by multiple customers with common goals/concerns or business
- Hybrid – any of the above

What is Virtualization ?

- Virtualization an old concept; mainframes have been using it since the 1980s
- Virtualization adds security and management complexities and risk to the environment
- The main mechanism of virtualization is the Hypervisor, the virtual machine manager which enables multiple hosts to run on the same physical hardware
- Hypervisors can run on the physical hardware directly (type 1) or on a host operating system (OS) running on the hardware (type 2)

Why use Virtualization ?

- Reduce costs by decreasing energy requirements and space with server consolidation
- Improve business continuity and provide high availability of applications by isolating critical applications on their own virtual machine and migrating virtual machines from one physical server to another
- Increase security by developing secure and standardized server images
- Faster deployment of virtual servers and applications
- Install multiple operating system technologies on a single hardware platform

Virtualization Security Risks

- Virtualization has introduced new security issues and vulnerabilities, specifically a wider attack surface including:
  - the hypervisor
  - a host OS (if running a type 2 hypervisor)
  - virtual networking
  - virtualization management system
- More difficult root cause analysis / investigations
- New skills and tools required; security and management practices may be overlooked in the process
- VM proliferation/forgotten images with access to data
- New types of attacks are targeting virtual infrastructure

Virtualization Attacks

- Hypervisor Escapes – attacker jumps from one guest virtual machine to another by exploiting or crashing the hypervisor
- Virtual Machine Attacks – miscreants delete virtual machine images and inject code into the virtual file structure
- Management Console Attacks – attackers leverage vulnerabilities to grab admin passwords or escalate to admin privileges
- Virtual Machine Migration – hackers change a virtual machine while it is being moved from one physical server to another
- Admin VM Attacks – denial of service by halting the admin VM or a tenant machine, grab clear text admin passwords, bypass authentication or inject malicious code
- Guest/Tenant Attacks – attackers crash the tenant virtual machine, install malware and thus gain admin privileges
- Hyperjacking – installing a rogue hypervisor to take control of the virtual infrastructure on the physical server. Known hyperjacking toolkits are BluePill, SubVirt and Vitriol

Cloud Security Risks:
Data is out of your direct control

- Data Segregation
  - How is your data protected from other tenants ?
- Recovery and availability
  - How does the provider maintain their SLA ?
- Privileged user management
  - How does the provider manage their sysadmin access ?
- Data Location
  - Where is your data stored—in a different country ?
- Compliance and regulatory requirements
  - They still apply; how do you ensure compliance ?
- Investigative support and discovery
  - Logs for customers may be comingled and spread across multiple data centers
- Vendor viability and stability
  - How will you retrieve your data/applications should the vendor fail

Mitigating Virtualization Risks

- Deploy centrally managed host based firewalls if extra protection is required for the data
- Use an add-on virtual security suite such as VMware's shield, Palo Alto, Juniper, Cisco’s VSG , Catbird or Hytrust to protect the hypervisor, virtual machine inter and intra machine traffic, virtual networks and guest host machines
- Isolate and protect the virtual infrastructure administrative and management functions using physical and virtual firewalls, VLANs, IDS/IPS, native virtual management authentication and authorization
- Protect the hypervisor using any native options within the hypervisor software
- Protect the guest machines using existing security standards: hardening the operating system/network stack and securing applications, patching and maintaining software
- Inventory and manage VMs: VMs no longer used should be deleted. This prevents unauthorized access to VM images and their data

Mitigating Cloud Risks

- If using an external cloud, you have no control over their choice of solutions to manage virtualization risks and management of the virtual infrastructure. What you can control is your choice of provider, and the following:
  - Encrypt sensitive data at rest and in transmission (and don’t store the keys in the cloud)
  - Consider that some data may be too sensitive to outsource
  - Ensure your provider is certified according to standards and complies with regulations your company is subject to
  - Strict control of admin IDs used to administer cloud services by your company staff
  - Take advantage of any extra security features or Identity and Access Management (IAM) services offered by the cloud provider

Summary

- Cloud services are an option for many companies, but its not a silver bullet for IT :
  - Time spent researching and talking to Cloud providers now will reap benefits for a secure, reliable , available and cost effective solution in the future
  - Virtualization adds another layer of security risk complexity to existing IT security issues
  - Virtualized data centers, whether within a company's site or at a cloud provider, require the same oversight, planning and management as a physical data center
  - Outsourcing to the cloud doesn't change regulatory culpability for your enterprise

Appendix

Standards and Regulations relevant to the Cloud

- ISO 27001
- NIST 800-53, SP800-125, SP800-146
- FEDRAMP
- PCI-DSS Cloud standards
- Cloud Security Alliance
- FISMA
- HIPAA
- SAS70
- COBIT
- Sarbanes-Oxley

A few Virtualization Security Products

- http://www.vmware.com/products/datacenter-virtualization/vcloud-network-security/overview.html
- http://www.juniper.net/us/en/products-services/security/vgw-series/
- http://www.cisco.com/en/US/products/ps11208/index.html
- http://www2.catbird.com/
- http://www.hytrust.com/

Cloud Working Groups

- https://www.oasis-open.org/committees/tc_cat.php?cat=cloud
- http://www.opengroup.org/getinvolved/workgroups/cloudcomputing
- https://cloudsecurityalliance.org/
- http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

Kaizen Approach and Cloud

- We have years of experience with evaluating vendors for services and setting up vendor management programs and risk management frameworks in the private sector: a key component for a successful cloud implementation
- We are familiar with existing regulations for compliance and standards for cloud and service providers
- We know security architecture and engineering; we apply those concepts to the virtual realm
- We are vendor neutral and not resellers
- We slice through the vendor hype and present facts

About Us

- Kaizen Approach, Inc. (KAI) is a certified Service-Disabled Veteran-Owned Small Business (SDVOSB)

- 91% of staff have TS/SCI with FSP clearances
- 82% have college degrees; 36% have Masters
- 55% of staff are certified; 27% have multiple certs

- To contact Kaizen Approach for more information on our services and offerings send an e-mail to info@KaizenApproach.com