Public Cloud Security: Surviving in a Hostile Multitenant Environment

SESSION ID: EXP-R01

Mark Russinovich
Technical Fellow
Windows Azure, Microsoft
@markrussinovich
The Third Computing Era

Security Could Hamper the Transformational Benefits of Cloud Computing
Survey: Data security concerns soar as more CPA firms access cloud

Cloud Adoption Hindered by Security Concerns, Survey Reveals

January 15th, 2014, 15:43 GMT | By Gabriela Volpe

By Jeff Drew
November 20, 2013

Concerns about data storage and security continue to increase as companies expand their use of cloud services.

Cloud services continue to face perception problems, with companies often believing they have security concerns when it comes to these services.

According to a global survey from the Interin Network, nearly 250 global Internet infrastructure decision makers were interviewed. They are part of a range of industries, including software and Internet hosting and are being asked whether they are currently using cloud services.

The survey also reveals that there is a significant difference in public cloud infrastructure concerns between the companies that are currently using such services and those that have no immediate plans to make the switch.

For the poll, nearly 250 global Internet infrastructure decision makers were interviewed. These are part of a range of industries, including software and Internet hosting.


Integration and governance while finding immediate solutions are major challenges for enterprises.
Concerns about public cloud hosting

Concerns about security and compliance with PCI and other standards in public cloud hosting environments remain high.

Level of concern:

- HIGH: 69%
- MEDIUM: 23%
- LOW: 8%

Source: 451 Research, Dec 2012
Goals of this Session

- Identify threats
- Discuss risk
- Explore mitigations
The Cloud Security Alliance “Notorious Nine”

- CSA periodically surveys industry experts to identify top cloud computing threats
- First report published in 2010
  - Seven top threats
- Most recent report published in February 2013
  - Nine top threats
  - So close to a top ten list…

https://cloudsecurityalliance.org/research/top-threats/
10. Shared Technology Issues: Exposed Software

- Some shared code defines the surface area exposed to customers:
  - CPU firmware/microcode
  - Hypervisor
  - Web server
  - API support libraries
  - ...
10. Shared Technology Issues

- What if there’s a vulnerability?
10. Shared Technology Vulnerabilities: The Enterprise Approach

- Stability and security are balanced against each other
- Assumes infrastructure is accessible only by trusted actors
- Corporate and legal mechanisms for dealing with attackers

Enterprise Multi-tenancy
10. Shared Technology Vulnerabilities: The Cloud Risk

- A vulnerability in publically accessible software enables an attacker to puncture the cloud
  - Breach exposes data of other customers
  - Single incident can cause catastrophic loss of customer confidence
  - Customers (potential attackers) are anonymous and in diverse jurisdictions
  - New bug classification: “Cloud Critical”

Hostile Multi-tenancy
10. Shared Technology Vulnerabilities: Bottom Line

- Enterprises and clouds are exposed to this risk
- Clouds are at higher risk of exploitation:
  - Data from many customers makes it a rich target
  - API surface is trivial to access
- Clouds are generally better at response:
  - Their business depends on it
  - Automated software deployment and patching required for cloud scale
  - Breach detection/mitigation necessary for preserving trust
9. Insufficient Due Diligence

- Many companies are moving to the cloud and side-stepping IT processes:
  - IT management, auditing, forensics, and access control systems are designed for on-premises servers and applications
  - Shadow IT: when business units bypass IT to deploy applications and store data in the cloud
- Bottom line:
  - IT must determine how to enable business units while enforcing corporate governance
  - IT must lead responsible adoption – it’s happening with or without them
8. Abuse of Cloud Services

- The agility and scale of the cloud is attractive to attackers, too
  - Use of compute as malware platform (Botmaster, DDOS platform)
  - Use of storage to store and distribute illegal content
  - Use of compute to mine digital currency
8. Abuse of Cloud Services: It’s Happening

- Attackers can use cloud resources and remain anonymous
  - Free trial offers
  - Stolen credit cards
  - Hijacked accounts
- Bottom line: reputation and COGS risk for cloud service providers
7. Malicious Insiders

- Many cloud service provider employees have access to cloud:
  - Developers that write cloud service code
  - Operators that deploy code
  - Datacenter operations personnel
7. Malicious Insiders

- **Mitigations:**
  - Employee background checks
  - Limited as-needed access to production
  - Controlled/monitored access to production services
- **Bottom line:** real risk that is better understood via third-party audit/certification
6. Denial of Service

- The public cloud is…well, public
  - Service endpoints are subject to DDOS attacks
  - Customer applications are subject to targeted DDOS

- Cloud outages are a form of DOS
6. Denial of Service: Bottom Line

- DOS is a significant threat
- Mitigations:
  - Cloud providers invest heavily in DDOS prevention
  - Non-public applications can be isolated from the Internet
  - Geo-available cloud providers can provide resiliency against many cloud outage vectors
5. Insecure Interfaces and APIs

- Cloud is new and rapidly evolving, so lots of new API surface
- Examples:
  - Weak TLS crypto
  - Incomplete verification of encrypted content
5. Insecure Interfaces and APIs

- **Bottom line:**
  - Cloud providers must follow SDL
  - Customers should validate API behavior
4. Account or Service Traffic Hijacking

- Account hijacking: unauthorized access to an account
- Possible vectors:
  - Weak passwords
  - Stolen passwords
  - Password reuse
4. Account or Service Traffic Hijacking: Cloud Infrastructure Threats

- Account hijacking is not specific to the Cloud, but:
  - Cloud use may result in unmanaged credentials
  - Publically accessible applications/services may allow for brute forcing
  - Applies to cloud provider: cloud support infrastructure is a back door
4. Account or Service Traffic Hijacking: Bottom Line

**Mitigations:**
- Turn off unneeded endpoints
- Strong passwords
- Two-factor authentication
- Breach detection
3. Data Loss

- There are multiple ways to lose cloud data:
  - Customer accidentally deletes or modifies it
  - Attacker deletes or modifies it
  - Cloud provider accidentally deletes or modifies it
  - Natural disaster destroys datacenter
3. Data Loss: Bottom Line

- **Mitigations:**
  - **Customer:** point-in-time backups matter, even in the cloud
  - **Customer:** geo-redundant storage
  - **Cloud Provider:** deleted resource tombstoning

![RISK MATRIX](image)
2. Data Breaches

- Really represents a collection of threats:
  - Insider threat, vulnerability in shared technology, etc.
- Ultimately, a company’s main asset is its data
- How does a company ensure its data is protected even in the face of successful breach?
  - Need to look at the threats individually…
2. Data Breaches: Physical Attacks on Media

- Threat: attacker gains access to media removed from datacenter
- Mitigation: cloud provider physical controls
- Enhanced mitigations:
  - Third-party certifications (e.g. FedRamp)
  - Encryption at rest
2. Data Breaches: Physical Attacks on Data Transfer

- **Threat:** attacker man-in-the-middle snooping on data links
- **Mitigations:**
  - Cloud provider encrypts inter-DC links
  - Cloud provider APIs use TLS
  - Customer uses TLS
  - Customer encrypts outside of cloud
2. Data Breaches: Side-Channel Attacks

- Threat: Collocated attacker can infer secrets from processor side-effects

https://www.cs.unc.edu/~reiter/papers/2012/CCS.pdf
2. Data Breaches: Side-Channel Attacks

- Researcher assumptions:
  - Attacker knows precise cryptographic code customer is using and key strength
  - Attacker can collocate on same server
  - Attacker VM shares same physical core as customer VM
  - Customer VM continuously executes cryptographic code
  - Other customers performing similar algorithms do not share physical core

- Bottom line: *not a risk in practice*
2. Data Breaches: Logical Attack on Storage

- Threat: attacker gains logical access to data
- Mitigations:
  - Defense-in-depth prevention
  - Monitoring/auditing
- Encryption-at-rest: not a significant mitigation
  - Assume attacker can use keys
2. Data Breaches: Bottom Line

- Media breach is not a significant risk
  - Encryption-at-rest doesn’t buy much
- Network breach is a risk
  - Encryption-on-the-wire is recommended
- Logical breach is a risk
  - Encryption-at-rest doesn’t buy much
1. Self-Awareness

Cloud Operations

DevOps

Deployer

Private Network

Internet

Attacker

Consumer

Enterprise

Private Network

Datacenter

Cloud Service Provider

Internet
The Top-10

1. Self-awareness
2. Data breaches
3. Data loss
4. Account or service traffic hijacking
5. Insecure interfaces and APIs
6. Denial of service
7. Malicious insiders
8. Abuse of cloud services
9. Insufficient due diligence
10. Shared technology vulnerabilities
Summary

- As with any new technology, there are new risks
- It’s our responsibility to educate our businesses and customers
- We can also develop tools and processes to mitigate risk