Everything You Need to Know About Cloud Security (and then some)

Mike Rothman
Securosis, L.L.C.
About Securosis

If you want someone to tell you how good you are, call your mom.
If you want to know how to build a security program, call us.

For more information, visit the Securosis website at www.securosis.com.
A long time ago...

You know, 2008
In a galaxy far far far away

You know, the Internet

(Where all the porn is)
These guys...
Said, “Hey, we need the next big thing.”
So this guy
Said....
“Hey, you know all those complicated diagram thingies customers are showing us?”
Like this?
Notice something?
They all have one of these
And I’ve never seen a customer with one, so let’s sell them *that*!
And thus THE CLOUD was born.
And there was much rejoicing.
Unless, of course, you were in IT security.
And your developers told you they moved everything to the cloud.
Last week.
In which case, it was more like this...
Why the cloud is a problem for security

- Poor understanding of cloud taxonomies and definitions.
- A generic term, frequently misused to refer to anything on the Internet.
- Lack of visibility into cloud deployments
- "IT by credit card" - Anyone can buy a cloud
Cloud Essential Characteristics

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service
- Resource Pooling
Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Essential Characteristics

Resource Pooling

Service Models

Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)

Deployment Models

Public
Private
Hybrid
Community
Three Delivery Models

- Software as a Service
- Platform as a Service
- Infrastructure as a Service
SPI Mix and Match

Amazon EC2
Salesforce.com CRM
Microsoft Azure
Database.com
Wordpress.com
DropBox

SaaS
PaaS
IaaS

Why?
Security Implications

• Variable control.
• Variable visibility.
• Variable simplicity.
• Variable resources.
Control, visibility, resources

Simplicity, manageability

Software as a Service

Platform as a Service

Infrastructure as a Service
Different Security Accountability

SaaS  PaaS  IaaS

Security Responsibility

Provider  Customer
But is the cloud more or less secure than we are now?
It depends
SaaS

• Most constrained.
• Most security managed by your provider.
• Least flexible.
PaaS

• Less constrained.

• Security varies tremendously based on provider and application - shared responsibility.

• Security responsibility
IaaS

- Most flexible.
- Most security managed by your developers and operations folks.
Specific issues

• Spillage and data security.
• Reliability/availability/Survivability.
• Relevance of traditional security controls in a dynamic environment.
• Lack of visibility into cloud usage.
• Changing development patterns/cycles.
For example, where do you stick the WAF?
Is vulnerability scanning your cloud legal?
How do you use your static and dynamic analysis testing tools in the cloud?
What is your DR/BC plan when the cloud fails?
More Risky Business...

- Data outside of your control
- Legal jurisdictions
- Service level definitions
- Monitoring/Visibility
- Incident response challenges
How most organizations secure their clouds today...
Your Top 2 Cloud Security Defenses

- Service Level Agreements
- Security Understanding
Understand Your SLAs

- Are there security-specific SLAs?
- Can you audit against those SLAs?
- Are there contractual penalties for non-compliance?
- Do your SLAs meet your risk tolerance requirements?
Suggested SLAs

- Availability.
- Security audits- including third party.
- Data security/encryption.
- Personnel security.
- Security controls (depend based on service).
- User account management.
- Infrastructure changes.
Understand Your Cloud

- What security controls are in your cloud?
- How can you manage and integrate with the controls?
- What security documentation is available?
- What contingency plans are available?
Cloud Security Controls to Look For

- Data encryption/security (key management).
- Perimeter defenses.
- Auditing/logging.
- Authentication
- Segregation.
- Compliance/Audits.
Don’t Trust

- SAS70 Audits.
- Documentation without verification.
- Non-contractual SLAs.
- Anything not in writing, with penalties for non-compliance.
- Anything you don’t understand.
Resources

- Cloud Security Alliance
- NIST
- ENISA
What to Do

- Educate yourself.
- Engage with developers.
- Develop cloud security requirements.
- Understand risk/controls tradeoffs.
- Document and engage management.
The 5 Stages of Cloud Computing Grief

• **Denial**: There is no cloud.

• **Anger**: Why the f&*k is this sales guy trying to sell me a cloud?

• **Bargaining**: Can you please just tell me what the f&^k your cloud is?

• **Depression**: The sales guy found my CIO. Now I have to buy a cloud.

• **Acceptance**: There is no cloud.
There is no cloud?
Read our stuff

- Blog: http://securosis.com/blog
- Content available via email
- Primary research
  - http://securosis.com/research
- We publish (almost) everything for free
- Contribute. Make it better.
Mike Rothman
Securosis LLC

mrothman@securosis.com
http://securosis.com
Twitter: @securityincite