Surviving the Cloud Computing

Dr Jamalul-lail Ab Manan
MIMOS Berhad

csm-ace 2013
CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION
13-14 November
The Royale Chulan, Kuala Lumpur

"SECURING CYBERSPACE FOR ECONOMIC GROWTH"
www.csm-ace.my

Innovation for Life™
Applied Research in Frontier Technologies

Problem Statement

- In cloud computing deployment, outages and data loss are bigger risks than security breaches to cloud subscribers;
- And enterprises are ill-prepared for this type of incident.
- What option do we have?

Panel Discussion

- Moderator:
  - YM Raja Azrina Raja Othman, Principal Consultant ICT Security, BT Malaysia
- Panelists:
  - Aloysius Cheang, Managing Director APAC, Cloud Security Alliance
  - Dr. Koji Nakao, Information Security Fellow and Distinguished researcher, NICT, Japan
  - Dr. Jamalul-lail Ab Manan, Principal Researcher, Strategic Advanced Research Cluster, Information Security Fellow and Distinguished Researcher MIMOS

The Issue

NETWORKWORLD News | Blogs | Newsletters | Videos | Events | Resources | INSIDER

Security | LANs & WANs | UC / VoIP | Cloud | Infrastructure Mgmt | Wireless | Software | Data Center | SMB

SaaS | White Papers | Webcasts | Tests

News

Gartner's state of cloud security: Outages are bigger risk than breaches

Outages by various cloud providers have been more common than security breaches, Gartner says, but few businesses are prepared for them

By Brandon Butler, Network World
November 14, 2012 02:52 PM ET

6 Comments Print Share 60 +1 More

Network World - Security remains a chief inhibitor to enterprise adoption of cloud computing resources and one Gartner analyst says the biggest concern should not be that data could be compromised in the cloud, but rather that there may be a cloud outage that could lead to data loss.

There's a perception, says Gartner cloud security analyst Jay Heiser, that the most significant risk in using the cloud is that sensitive data can be leaked. But there's been little evidence of that, he says. Sony suffered a compromise of potentially tens of millions of customers in 2011 related to its cloud, and there have been a handful of other breaches of personally identifiable information being leaked from the cloud.

But more common nowadays are cloud outages and data loss, and Heiser says many enterprises are ill-prepared for those incidents.

csm-ace 2013
CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION
13-14 November
The Royale Chulan, Kuala Lumpur

Cloud Computing has a good prospect.

- Big market opportunity. Cloud Service Provider is the key to its success.
  - However, which provider do you trust?
  - How to get a good Cloud Service Provider.
- **But Cloud Computing Deployment has two major issues**
  - Issue: Outages & Data Loss – big risks – Enterprises are ill prepared for this– lack of Business Continuity Process (BCP)
  - Issue: Security Breaches to cloud subscribers (customers) – lost or stolen identity – No user control of their private data
- **What options do we have??**

Threats

- Threats to Enterprise and Customers
  - Threats to Enterprise from hackers and surveillance
    - Customer Data Losses or leakages
    - Advanced Persistent Threat (APT) i.e. threats to root administrators,
    - Constant surveillance by foreign states (e.g. NSA).
    - Lose reputation and business
- Threats to Customers from hackers and surveillance
    - Individual Identity and data loss

Security and Trust

- **Security may still be a major problem**
  - **Cloud Customers**
    - **Encryption is easily cracked if <128 bits, customers lose identity and data**
    - **Currently, cracking password using GPU in 30 nsec.**
  - **Cloud Network Providers**
    - **Those who sell network security systems could find hackers getting into their systems**

Security and Trust

- **Trust is another big issue**
  - **Cloud Customers**
    - **Untrusted Service Providers could gather personal data, company data, etc.**
  - **Cloud Service Providers**
    - **Untrusted Components of Cloud/Infrastructure could lead to data leakage**

Privacy

- **Privacy is a big issue**
  - **Cloud Integrity**
    - **Main issue raised by all sectors**
    - **Preventing crime is often difficult, detecting crime is manageable**
  - **Cloud Customers**
    - **Stolen Identities and Information**
    - **Depends on who you are talking to e.g. some are terrified and worried**
    - **Individuals, institutions – both worried about the right to personal information protection (privacy)**
    - **Individuals – privacy breach – can also lead to individual sabotage.**
  - **Cloud Service Providers**
    - **Depends on service – access to virtual machines (Cloud) is still very open privacy issues**
    - **Patriot in Europe – databases / storage can be broken through untrusted VM in Cloud Storage**

Secure Trusted and Privacy Enhanced Cloud

How can we build a Secure Trusted and Privacy Enhanced Cloud?

- Technology
  - Security & Privacy Enhancing Technology
    - Keyless signature – ongoing research
    - Key management, especially for devices and IoTs
    - Semantic Security
    - Homomorphic encryption – ongoing research
  - Trusted Computing
    - Trusted cloud framework, Trusted Network Connect (TNC) , Network Access Control and Security Automation
    - Trusted Compartments / Trusted Virtual Domains (TVD)s

Cloud Provider

Cloud Provider – What do we look for?

- How do we build a Trusted Cloud for Service Providers
  - Complete Framework for Technology and Legal
    - Technology Framework for Trusted Cloud
      - Cloud Trust Protocol by Cloud Security Alliance (CSA)
    - Legal Framework for Trusted Cloud Computing
      - Legal / Law and Policy Enforcement/ Audit Control
  - Complete Architect the cloud computing
    - Open Architecture with security, trust and privacy built-in
    - TNC open architecture using Trusted Computing
    - Trusted Data Center
  - Complete Architecture for Applications
    - Trusted Application in Compartments (Trusted Virtual Domains)
    - Integrity Verifications for all critical components
    - User Application Data must be protected (sealed using HW assisted means)
    - Choices for users to store and retrieve which private data

Customer

Customer: How do we survive the Cloud Computing?

- Options for Customers:
  - Comply with international security, trusted computing and privacy standards
  - Use security compliant components
  - Use Trusted Virtual Domain technology
  - Use Privacy Enhancing solutions
  - Use more open source technology to avoid back door

Thank You

Email: jamalul.lail@mimos.my

Innovation for Life™

Applied Research in Frontier Technologies

Cloud Advantages and Disadvantages

Disadvantages	Advantages
Privacy	Thin Client
Reliability	Update Speed
Migration	Cost Savings
Legal	HW/SW Independence
Account Security	Server Security
Lock in	

Ref: Demystifying the Clouds: A survey of Cloud Computing, Jesse Dunietz, SASS Talk