Deloitte.

Cloud Forensics

The more things change, the more they stay the same.

Michael Köhn
Cyber Security Lab

Presentation Structure

- Cloud Computing
- Digital Forensics
- Cloud Forensics
- Isolating a Cloud Instance for a Digital Forensics Investigation
- Practical Application
- Cloud Forensics Panic

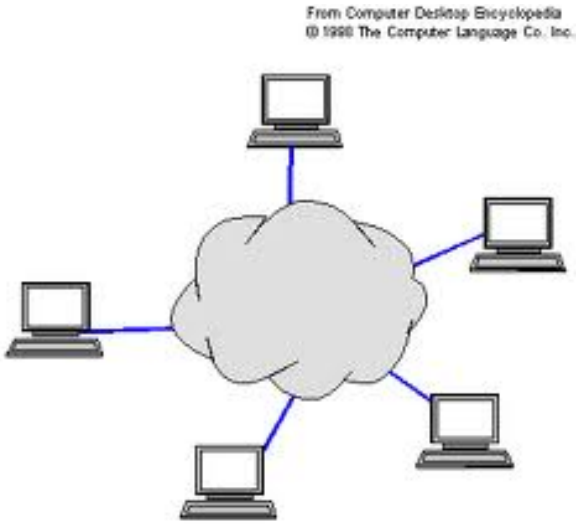
Cloud Computing

Defined

- Use of Computing Resources, both hardware and software;
- Where services are delivered over a network, typically the Internet;
- Extensive use of user data, software and computation via remote services.

- Public cloud computing typically includes:
  - Infrastructure services – Corporate world moving into this space
  - Platform services – extension of desktop virtualisation
  - Software Services – incorrectly, Google OS
  - Storage services - Dropbox
  - Security services - hmmm
  - Data as a service – been around for some time as Databases
  - Test environments – development testing
  - Desktop services – why even have an operating system?

Cloud Computing Architecture



- Cloud Clients – browser and mobile applications
- Application Layer – Email and virtual desktops
- Platform – Database, web server, dev tools and Runtime environments
- Infrastructure – VMs, servers, storage, load and network.

Cloud Computing

Opinion

"People are coming to grips with Virtualization and how it reshapes IT, creates service and software based models, and in many ways changes a lot of the physical layer we are used to. Clouds will be the next transformation over the next several years, building off of the software models that virtualization enabled."

Douglas Gourlay

"I view cloud computing as a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a 'pay-as-you-go' basis that previously required tremendous hardware/software investments and professional skills to acquire. Cloud computing is the realization of the earlier ideals of utility computing without the technical complexities or complicated deployment worries."

Jeff Kaplan

Digital Forensics

Defined

- a specific, predefined and accepted process
- applied to digitally stored data or digital media
- using scientific proven and derived methods,
- based on a solid legal foundation,
- to produce after the fact digital evidence with the goal of deriving the set of events or actions
- indicating a possible root cause,
- where reconstruction can be used to validate the scientifically derived conclusions

Digital Forensics

Process

- identify, collect, preserve, transport, store, analyse, interpret, attribute, reconstruct, present, destroy (cohen)
- organisations involved in DF must have a specific process to execute when Digital Evidence is being questioned
- Process not always clear-cut
- Scientific proven (Daubert and Fray)
- Root cause or not - know what to look for

Digital Forensics

Daubert Standard

Empirical testing where the theory or technique must be falsifiable, refutable, and testable.

1. Subjected to peer review and publication.
2. Known or potential error rate.
3. The existence and maintenance of standards and controls concerning its operation.
4. Degree to which the theory and technique is generally accepted by a relevant scientific community.

Cloud Forensics

Combination of Digital Forensics and Cloud Computing

Cloud Computing crimes poses unique forensics challenges

- Where is the data?
- Can it be Collected?
- What are the Challenges?

“Forensics in the cloud is not necessarily a new field, but requires a new skill set and being able to learn on the fly," says Rob Lee, curriculum lead for digital forensic training at SANS Institute. "Their strength will be in assuring that they get that information and data out in a manner that is sufficient for their forensic need.”

"Cloud forensics is difficult because there are challenges with multi-tenant hosting, synchronization problems and techniques for segregating the data in the logs," said Keyun Ruan, a PhD candidate at the Centre for Cyber Crime Investigation in Ireland. "Right now, most of the cloud service providers are not open to talking about this because they don't know the issues."

Isolating a Cloud Instance for a Digital Forensics Investigation – Paper available online

Some thoughts:

- Companies rely heavily on Cloud services, are they aware of the security risks?
- Multiple instances can be contained in a single node, is your data exclusive to that node?
- Can your investigation data, evidence, be isolated securely for a Cloud Forensics Investigation?

Possible solutions, at great cost:

Server farming

Instance relocation

Address relocation

Sandboxing

Man in the Middle

Let's hope for the best

Practical Application

Some Examples

- Social networking – Twitter, Facebook, WhatsApp, Youtube, LinkedIn, BBM and Mxit
- Email – Gmail, IBM LotusLive iNotes, Microsoft Exchange, Cisco WebEx Mail, PanTerra Networks, mimecast

Challenges

- Information Spread
- Volumes of data increasing
- Effect and Speed
- Fact v Fiction
- Jurisdiction
- Privacy
- Porthole password – do you don't you, can you, cant you?

Cloud Forensics Panic

2 Examples

Microsoft Exchange -

Mimecast –

Slide is complete!

I want to hear what you say?

Think – because you have to be the one being forensically ready in case of an investigation.

Questions?

Michael Köhn

mkohn@deloitte.co.za

0834577112


Deloitte.