itrust consulting

iT Days 2014

21/03/2014

Dr. Carlo HARPES

Forensics and preventing anti-forensics on data leakage with/without cloud services

itrust consulting s.à r.l.
6 Z.I. Bombicht
L-6947 Niederanven

Tel: +352 26 176 212
Fax: +352 26 710 978
Web: www.itrust.lu

Motivation

Cloud computing threats

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service & Traffic Hijacking
7. Unknown Risk Profile

\+

How do you find out what happened to your data?

Agenda

- Basics on forensic analysis
- Additional challenges for cloud services
- Preventing Anti-Forensics

Basics of forensic analysis

The most important thing:

Keep evidence!

Preserve Non-repudiation!

Document everything you do, with witnesses.

Rely on (independent) experts.

Basics of forensic analysis

The most important thing:

DO NOT TOGGLE THE STATE OF THE DEVICE

If the device is on => do not turn it off

If the device is off => do not turn it on

Basics of forensic analysis

Timeline of a forensic analysis

Source: itrust consulting

Basics of forensic analysis

Live Forensics vs. Post-Mortem Forensics

Live Forensics	Post-Mortem Forensics
Often volatile data	Mostly **no** volatile data
Device is turned on	Device is turned off
Information Gathering at place	Information Gathering in the lab
Working on the live system	Bit-by-Bit copy possible
Large amounts of data can be handled	Risk to need **much** disk-space

Additional challenges for cloud services

Meta-Data

- Examples of document meta-data:
  - name, size, date of creation, author, file type…..
- Examples of network connection meta-data:
  - Destination IP, Source IP, timestamp, protocol….
- Main task of forensic analysis = analysis of meta-data

Additional challenges for cloud services

Interdisciplinary

- Use other investigations, inquiries
  - Use info and meta-data to get real data.
- Use legal advice:
  - Destination IP, Source IP, timestamp, protocol….
- Collaborate with forensics by Police
  - Other possibilities, better credibility in court, different tools
  - No control, slow…

Additional challenges for cloud services

Public Clouds

- Several legal restrictions
- Several technical difficulties
- In most cases: less information is available

Preventing Anti-Forensics

By internal staff:

- Forbid BYOD
- Set Security objectives and rules (formally agreed by all staff)
- Forbid TrueCrypt, Bitlocker etc. or…

  … unless key escrow
- Use dedicated Faraday envelopes to prevent remote wiping
  - If not possible, set smartphone to airplane-mode
  - 5-7€ / envelope

Preventing Anti-Forensics

In general:

- Do regular Pentests to avoid the need for forensics
- Do regular Backups (servers, clients, logfiles, smartphones)
- Set up dedicated Log-Servers
- Nobody shall be able to manipulate your log, otherwise useless in court.

Preventing Anti-Forensics

In the cloud, how do you detect and investigate against data leakage?

- It's very hard!
- Take care of your cloud contracts (right to audit, transparency on processing, access to security incident information)
- Encrypt, anonymise, etc., but consider the value of meta-data.

Recur to specialised Security Consultants for further help…

itrust consulting

Any questions?

Thank you for your attention