FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Forensische Untersuchungen in der Computer Cloud

Tobias Esser
Lehrgebiet Datennetze

IT Forensik
FH Aachen

Gliederung

- Aufgabestellung
- Motivation
- Grundlagen
- Umsetzung
- Ergebnisse
- Fazit

Aufgabenstellung

In dieser Arbeit soll die Technik von Cloud Computing und deren Auswirkung auf eine forensische Untersuchung dargestellt werden:

- Was ist noch möglich?
- Wie kann überhaupt noch untersucht werden?
- Welche Hilfsmittel gibt es?
- Nicht im Fokus: Rechtliche Aspekte! Was darf man?

Motivation

- Cloud Computing extrem wachsender Markt
- Bedarf an forensischer Software/Methodologie
- Keine einheitliche Vorgehensweise/Richtlinien
- Die Cloud als Tatort oder als Angriffswerkzeug

Grundlagen

- Definition nach NIST

*"**Cloud computing** is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

- Shared pool
  - Physische Infrastrukturen werden mit anderen Benutzern geteilt
- Configurable computing resources
  - Für den Benutzer frei konfigurierbar
- Minimal management
  - Schnelle Erstellung, ohne viel Aufwand

Cloud Liefermodelle

- Private
  - Exklusive Nutzung für eine einzelne Organisation
- Public
  - Öffentlich, keine Wartung
  - Hohe Skalierbarkeit
- Hybrid
  - Benutzung von Private und Public
- Community
  - Mehrere Unternehmen teilen sich Private Cloud

Cloud Servicemodelle

- IaaS (Infrastructure as a Service)
  - Virtuelle Infrastruktur
  - Beispielanbieter: Amazon EC2, Nimbula
- PaaS (Plattform as a Service)
  - Virtuelle Betriebssysteme
  - Beispielanbieter: Windows Azure, Google App Engine
- SaaS (Software as a Service)
  - Virtuelle Software
  - Beispielanbieter: Google Docs, Salesforce

In meiner Arbeit Untersucht

1. Forensik in der Privaten Cloud
   - Microsoft
2. Infrastructure as a Service Forensik
   - Amazon EC2 Service
3. Plattform as a Service Forensik
   - Windows Azure
4. Software as a Service Forensik
   - Salesforce

1. Forensik in der Privaten Cloud

- Vorteile
  - Zugriff auf physische Hardware
  - Kontrolle über Tools die Daten gesichert haben

- Cloud erstellt mit Microsoft Produkten

1. Forensik in der Privaten Cloud

- Daten sichern

  - Zugriff auf VHD Files
  - Snapshots
  - Monitoring Tools
  - Netzwerkmitschnitte

VHD: **V**irtuel **H**ard **D**isk. Speicherort der virtuellen Maschinen.

1. Forensik in der Privaten Cloud

- Daten analysieren
  - Analyse der VHD Files/Snapshot mittels X-Ways o.ä.
    - Daten wiederherstellen
    - Timeline – Analyse
  - Analyse Logfile von Monitoring Tools
    - Angemeldete Nutzer
  - Netzwerkmitschnitte
    - „kommt noch“

In meiner Arbeit Untersucht

1. Forensik in der Privaten Cloud
   - Microsoft
2. Infrastructure as a Service Forensik
   - Amazon EC2 Service
3. Plattform as a Service Forensik
   - Windows Azure
4. Software as a Service Forensik Forensik
   - Salesforce

2. Infrastructure as a Service Forensik

- Vorteile
  - Zugriff auf virtuelle Machine

- Nachteile
  - Keine 100% Sicherheit korrekte Daten gesichert zu haben
    - Abhängig von Anbieter
  - Enorme Datenmengen
    - Sicherung über Internet

- Untersuchungen an Amazon EC2
  - Bekanntester Anbieter

2. Infrastructure as a Service Forensik

- Daten sichern
  - Live Response
    - Flüchtige Daten sichern
    - Herkömmliche Tools (PSTOOLS)
    - Windows-eigene Tools (über Netzlaufwerk gestartet)

```
2  ipconfig /all >Z:\ForensicTools2\results\ipconfigAll.txt
3  md5sum Z:\ForensicTools2\results\ipconfig.txt > Z:\ForensicTools2\results\ipconfigAll.txt
4
5  pslist > Z:\ForensicTools2\results\pslist.txt
6  md5sum Z:\ForensicTools2\results\pslist.txt > Z:\ForensicTools2\results\pslistHASH.txt
7  psservice > Z:\ForensicTools2\results\psservice.txt
8  md5sum Z:\ForensicTools2\results\psservice.txt > Z:\ForensicTools2\results\psserviceHASH.txt
9
10 pslist > Z:\ForensicTools2\results\pslist.txt
11 md5sum Z:\ForensicTools2\results\pslist.txt > Z:\ForensicTools2\results\pslistHASH.txt
12 md5sum Z:\ForensicTools2\results\psfile.txt > Z:\ForensicTools2\results\psfileHASH.txt
13 psinfo > Z:\ForensicTools2\results\psinfo.txt
14 md5sum Z:\ForensicTools2\results\psinfo.txt > Z:\ForensicTools2\results\psinfoHASH.txt
15
16 netstat -ano > Z:\ForensicTools2\results\netstatANO.txt
17 md5sum Z:\ForensicTools2\results\netstatANO.txt > Z:\ForensicTools2\results\netstatANOHASH.txt
18 netstat -rn > Z:\ForensicTools2\results\netstatRN.txt
19 md5sum Z:\ForensicTools2\results\netstatRN.txt > Z:\ForensicTools2\results\netstatRNHASH.txt
```

Abbildung: Ausschnitt von BATCH Datei mit Programmen, die über ein Netzlaufwerk ausgeführt werden

PSTOOLS:
http://technet.microsoft.com/de-de/sysinternals/bb896649

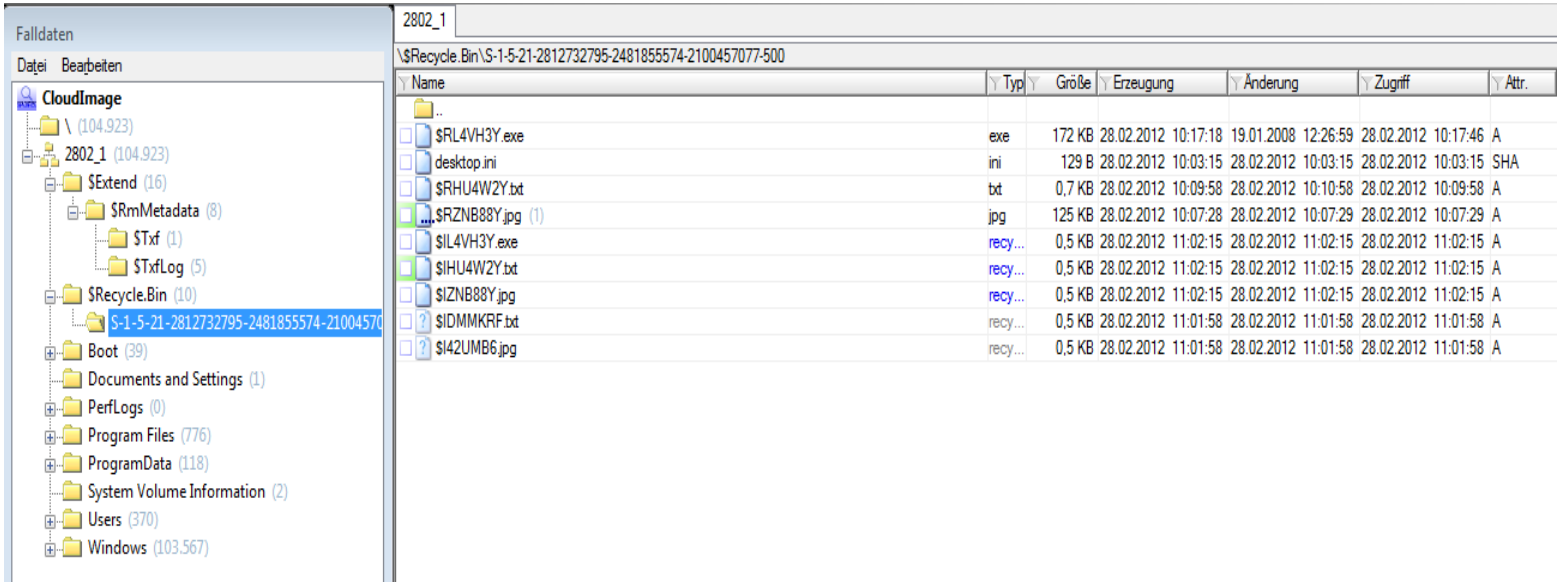
2. Infrastructure as a Service Forensik

- Daten sichern
  - Snapshots
    - Mit Tool von Amazon
  - Dump von Instanzen
    - Mit DCFLDD
  - Monitoring Tools
    - Amazon-eigene Monitoring Tools

DCFLDD: Vom **D**efense **C**omputer **F**orensics **L**ab weiterentwickelte **DD** Version. **http://dcfldd.sourceforge.net/**

2. Infrastructure as a Service Forensik

- Daten analysieren
  - Instanz-Dump mittels X–Ways o.ä.
    - Daten wiederherstellen
    - Timeline – Analyse



2. Infrastructure as a Service Forensik

- Daten analysieren
  - Live Response
    - Angemeldete Benutzer
    - Netzwerkdaten
    - Offene Dateien
    - Programme im Speicher
  - Snapshot mittels forensischer EC2 Instanz
    - Untersuchung auf EC2 Forensikinstanz

In meiner Arbeit Untersucht

1. Forensik in der Privaten Cloud
   - Microsoft
2. Infrastructure as a Service Forensik
   - Amazon EC2 Service
3. Plattform as a Service Forensik
   - Windows Azure
4. Software as a Service Forensik Forensik
   - Salesforce

3. Plattform as a Service Forensik

- Nachteil
  - Zugriff auf virtuelle Betriebssysteme
  - Keine 100% Sicherheit korrekte Daten gesichert zu haben
  - Vertrauen in Anbieter
- Untersuchungen an Microsoft Azure
  - OS von Microsoft Cloud-Platform
  - Besonders geeignet für Entwickler

3. Plattform as a Service Forensik

- Daten sichern
  - Azure eigene Diagnostic API
    - IIS 7 log
    - Crash dumps
    - Windows Events
  - Zugriff mittels Remotedesktop
    - Noch offen

IIS 7: Microsoft **I**nternet **I**nformation **S**ervices. Verwaltung für Dokumente und Dateien im Netzwerk

3. Plattform as a Service Forensik

- Daten analysieren

In meiner Arbeit Untersucht

1. Forensik in der Privaten Cloud
   - Microsoft
2. Infrastructure as a Service Forensik
   - Amazon EC2 Service
3. Plattform as a Service Forensik
   - Windows Azure
4. Software as a Service Forensik Forensik
   - Salesforce

4. Software as a Service Forensik

- Nachteile
  - Nur noch Zugriff auf Client
  - Keine 100% Sicherheit korrekte Daten gesichert zu haben
  - Vertrauen in Anbieter
- Untersuchungen an Salesforce
  - Größter SaaS Anbieter
  - Kundenbeziehungsmanagement

4. Software as a Service Forensik

- Daten sichern
  - Logfiles
    - Login Logs

Benutzername	Anmeldezeit	Quellen-IP	Anmeldetyp	Status	Browser	Plattform	Anwendung
t-esser@hotmail.de	13.04.2012 11:37:28 MESZ	149.201.22.113	Anwendung	Erfolg	IE 8	Win7	Browser
t-esser@hotmail.de	13.04.2012 11:37:20 MESZ	149.201.22.113	Anwendung	Ungültiges Kennwort	IE 8	Win7	Browser
chras_@hotmail.de	13.04.2012 11:34:04 MESZ	149.201.22.113	Anwendung	Erfolg	Firefox 11	Win7	Browser

    - Debugging Tools

Kategorie	Ebene	Ereignisse
Datenbank	INFO	SOQL_EXECUTE_BEGIN; SOQL_EXECUTE_END; SOSL_EXECUTE_BEGIN; SOSL_EXECUTE_END; QUERY_MORE_ITERATIONS; DML_BEGIN; DML_END; SAVEPOINT_SET; SAVEPOINT_ROLLBACK;
Workflow	INFO	WF_RULE_INVOCATION; WF_APPROVAL; WF_FIELD_UPDATE; WF_SPOOL_ACTION_BEGIN; WF_ACTION; WF_FORMULA; WF_RULE_EVAL_BEGIN; WF_RULE_EVAL_END; WF_RULE_EVAL_VALUE; WF_CRITERIA_BEGIN; WF_CRITERIA_END; WF_RULE_ENTRY_ORDER; WF_RULE_NOT_EVALUATED; WF_RULE_FILTER; WF_ESCALATION_RULE; WF_ESCALATION_ACTION; WF_TIME_TRIGGERS_BEGIN; WF_TIME_TRIGGER; WF_ACTIONS_END; WF_ENQUEUE_ACTIONS; WF_APPROVAL_SUBMIT; WF_APPROVAL_REMOVE; WF_NEXT_APPROVER; WF_EVAL_ENTRY_CRITERIA; WF_NO_PROCESS_FOUND; WF_SOFT_REJECT; WF_HARD_REJECT; WF_PROCESS_NODE; WF_ASSIGN; WF_REASSIGN_RECORD; WF_RESPONSE_NOTIFY; WF_OUTBOUND_MSG; WF_ACTION_TASK; WF_EMAIL_ALERT; WF_EMAIL_SENT; SLA_PROCESS_CASE; SLA_NULL_START_DATE; SLA_EVAL_MILESTONE; SLA_END; WF_KNOWLEDGE_ACTION;
Validierung	INFO	VALIDATION_RULE; VALIDATION_FAIL; VALIDATION_PASS; VALIDATION_ERROR; VALIDATION_FORMULA;
Callouts	INFO	CALLOUT_REQUEST; CALLOUT_RESPONSE;
Apex-Code	DEBUG	BULK_COUNTABLE_STATEMENT_EXECUTE; EXCEPTION_THROWN; METHOD_ENTRY; METHOD_EXIT; CONSTRUCTOR_ENTRY; CONSTRUCTOR_EXIT; EMAIL_QUEUE; FATAL_ERROR; VF_APEX_CALL; VF_PAGE_MESSAGE; ENTERING_MANAGED_PKG; HEAP_DUMP;
Apex-Profiling	INFO	CUMULATIVE_LIMIT_USAGE; CUMULATIVE_LIMIT_USAGE_END; TESTING_LIMITS;
Visualforce	INFO	VF_SERIALIZE_VIEWSTATE_BEGIN; VF_SERIALIZE_VIEWSTATE_END; VF_DESERIALIZE_VIEWSTATE_BEGIN; VF_DESERIALIZE_VIEWSTATE_END;
System	DEBUG	SYSTEM_METHOD_ENTRY; SYSTEM_METHOD_EXIT; SYSTEM_CONSTRUCTOR_ENTRY; SYSTEM_CONSTRUCTOR_EXIT; SYSTEM_MODE_ENTER; SYSTEM_MODE_EXIT; PUSH_TRACE_FLAGS; POP_TRACE_FLAGS;

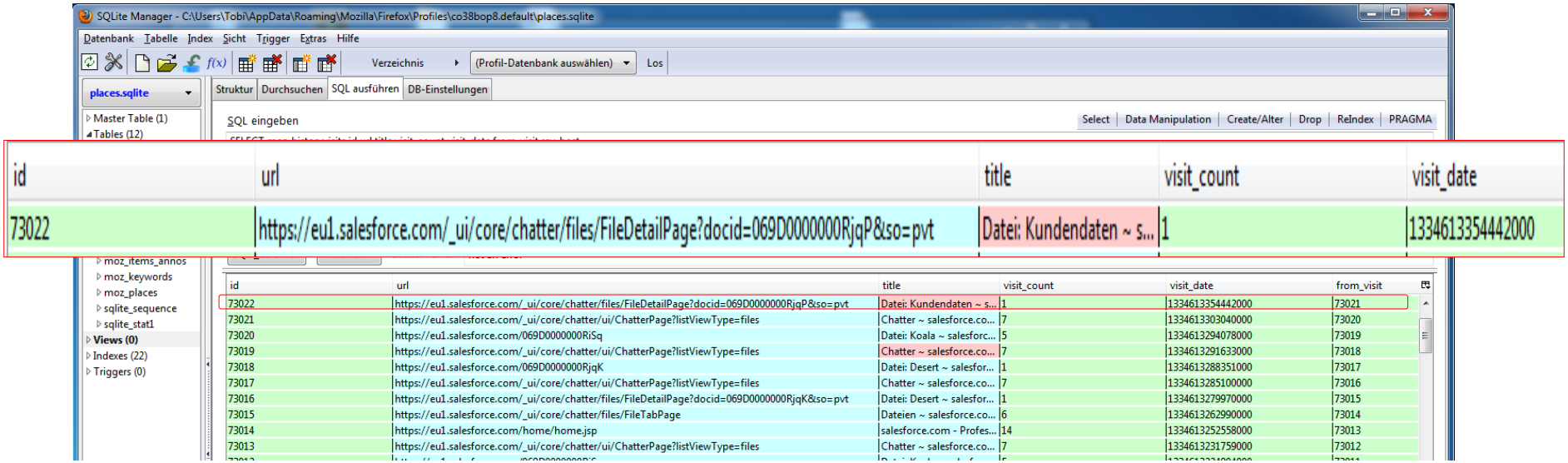
4. Software as a Service Forensik

- Daten sichern (Fortsetzung)

  - Client
    - z.B. Browser
  - Heap Dumps
    - Noch offen

4. Software as a Service Forensik

- Daten analysieren
  - Debug Logs auswerten
  - Browser History Datenbank analysieren



Fazit

	Private	IaaS	PaaS	SaaS
Physischer Zugriff	✔	✘	✘	✘
Dump von Instanz	✔	✔	-	✘
Logfiles	✔	✔	✔	✔
Timeline – Analyse	✔	✔	-	-
Live Response	✔	✔	-	✘

- ✔ : Bearbeitet
- ✘ : Nicht möglich
- - : Noch offen

Fazit

- Abhängig von Servicemodell
- Abhängig von Cloudanbieter
- Anbieter zeigen zu wenig Transparenz
- Noch keine Tools speziell für die Cloud

Fragen

Fragen?