Cloud Computing
Risiken und Massnahmen

Marc Ruef
www.scip.ch
)SCIP(

Datenschutz-Forum
22. November 2011
Zürich, Schweiz

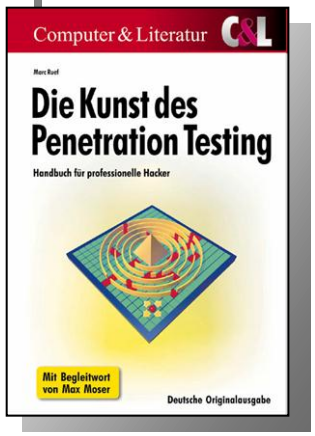
INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS | T +41 44 404 13 13 | F +41 44 404 13 14
BADENERSTRASSE 551 | 8048 ZÜRICH
)SCIP(

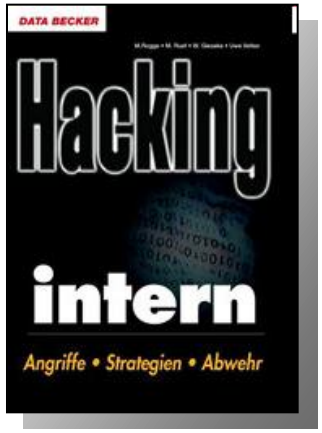
Agenda | Cloud Computing

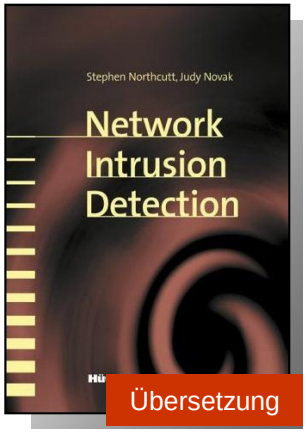
◦ Einführung	2 min
◦ Was ist Cloud Computing	2 min
◦ Implementierungen	5 min
◦ Sicherheitsprobleme	10 min
◦ Zusammenfassung	2 min
◦ Fragen	4 min

Einführung | Wer bin ich

Name	Marc Ruef
Beruf	Mitinhaber / CTO, scip AG, Zürich
Private Webseite	http://www.computec.ch
Letztes Buch	„Die Kunst des Penetration Testing“, Computer & Literatur Böblingen, ISBN 3-936546-49-5





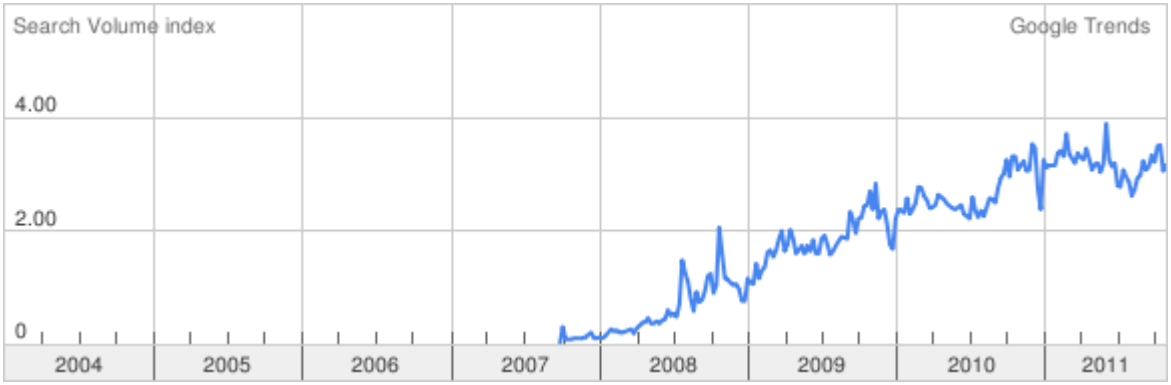


Intro
- Wer?
- Was?

Risiken
- Transparenz
- Vermengung
- Kontrolle
- Backup/Restore
- Abhängigkeit
- Migration
- Jur. Konflikte
- Verantwortung
- Knowhow
- Zentralisierung

Abschluss
- Zusammenfassung
- Fragen

Einführung | Aus dem Hype wird ein Trend



Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Einführung | Definition von Cloud Computing

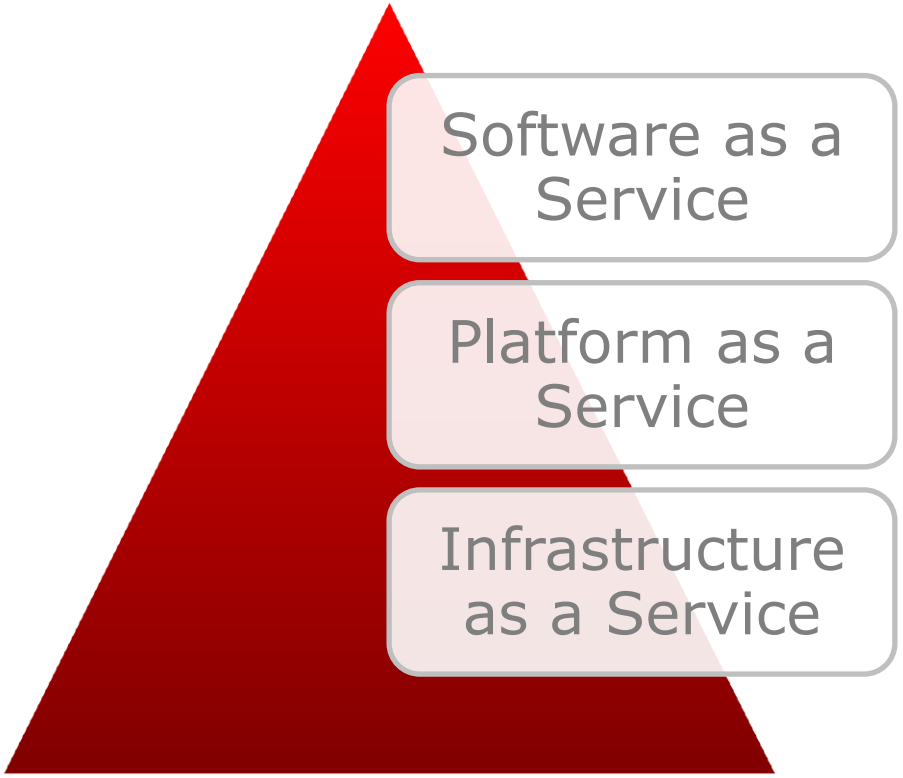
> *„[Cloud Computing ist] ein modulares System, in dem für Nutzer die Ressourcen transparent sowie dynamisch zugewiesen, verarbeitet und verrechnet werden."*
>
> – scip AG

Intro
- Wer?
- Was?

Risiken
- Transparenz
- Vermengung
- Kontrolle
- Backup/Restore
- Abhängigkeit
- Migration
- Jur. Konflikte
- Verantwortung
- Knowhow
- Zentralisierung

Abschluss
- Zusammenfassung
- Fragen

Einführung | Vertriebsmodelle

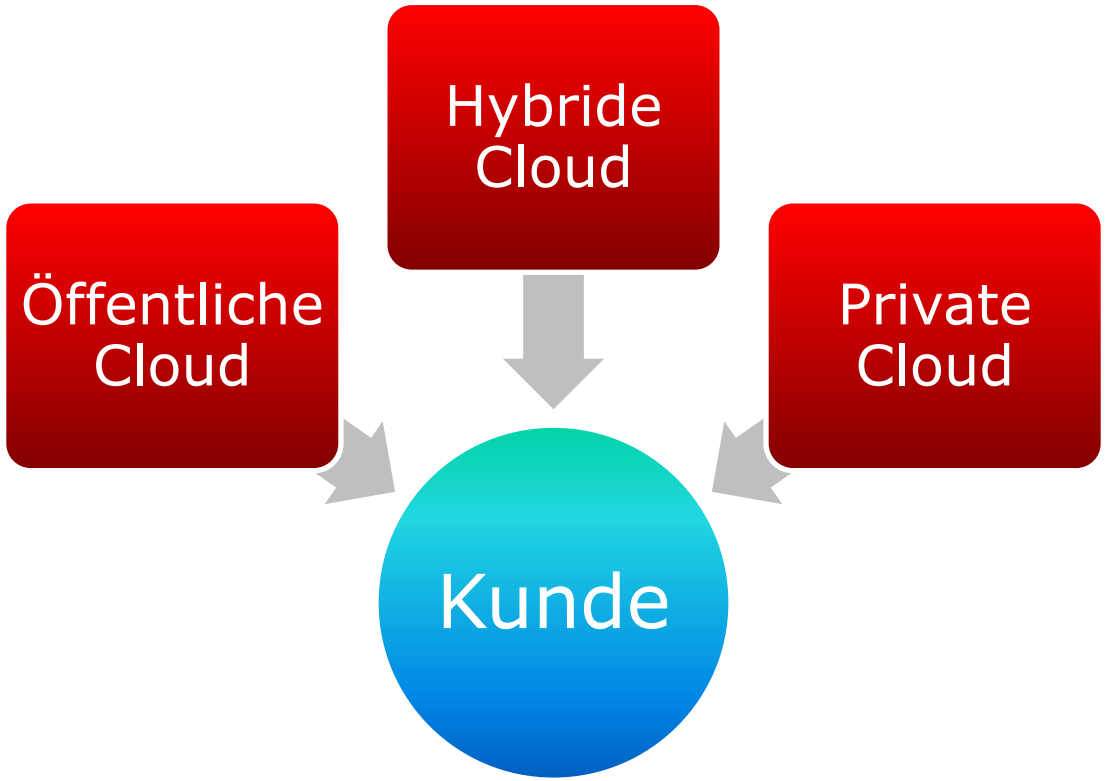


Intro
- Wer?
- Was?

Risiken
- Transparenz
- Vermengung
- Kontrolle
- Backup/Restore
- Abhängigkeit
- Migration
- Jur. Konflikte
- Verantwortung
- Knowhow
- Zentralisierung

Abschluss
- Zusammenfassung
- Fragen

Einführung | Infrastrukturmodelle



Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Fehlende Transparenz

- Unbekannte
  - Prozesse
  - Abläufe
  - Vorgaben
  - Umsetzungen
  - Abnahmen
  - Sicherheit
  - …
- Beispiel Fragen:
  - Werden Versprechen eingehalten?
  - Ist die gewährte Sicherheit annehmbar?

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Vermengung von Objekten

Haben keine Hardware mehr. Lass mal ein paar Kunden auf der *gleichen* Maschine laufen!

- Branchen
  - Finanzunternehmen
  - Behörden
  - Industrie
  - …
- Kunden
  - Bank Swiss AG
  - Bank USA Ltd.
  - Banque France SA
  - …
- Datentypen
  - Öffentliche Daten
  - Interne Daten
  - Kundendaten
  - …

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Verlust der Kontrolle

- Weiterverarbeitung
  - Unternehmensdaten
  - Mitarbeiterdaten
  - ...
- Weitergabe
  - Persönliche Daten
  - Statistische Daten
  - ...
- Weiterverkauf
  - Kundeninformationen
  - Geschäfts-geheimnisse
  - ...

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Backup und Restore

- Keine klaren, einheitlichen, offenen Schnittstellen
- Eigene Prozesse bleiben erforderlich
- Komplexe Anbindung möglich

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Abhängigkeit vom Anbieter

- Präsenz
  - Existenz (Insolvenz)
  - Lokation (Wegzug)
  - Erreichbarkeit
- Preise
  - Aufwand
  - Ressourcen
  - Spesen
- Arbeit
  - Angebot
  - Umfang
  - Qualität

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Schwierigkeit bei Migration

- Eventuell fehlende Unterstützung durch den Partner
- Inkompatible Mechanismen
- Mangelhafte Deckungsgleichheit unterschiedlicher Angebote

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

INFO@SCIP.CH
SECURITY • CONSULTING • INFORMATION • PROCESS | T +41 44 404 13 13 | F +41 44 404 13 14
BADENERSTRASSE 551 | 8048 ZÜRICH
)SCIP(

Risiken | Juristische Konflikte

- z.B. Datenschutz muss gewahrt bleiben (DSG)
- Unterschiedliche nationale Gesetzgebungen
  - Data Protection Act 1998 UK
  - Privacy Act of 1974 USA
- Länderübergreifende Abkommen
  - Europäische Datenschutzkonvention
- Internationale Rechtshilfebegehren
  - langwierig
  - komplex
  - aufwendig

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Juristische Eigenverantwortung

- Das Unternehmen bleibt trotzdem haftbar für:
  - Vorgaben
  - Richtlinien
  - Prozesse
  - Abläufe
  - Angebote
  - Daten
  - Infrastruktur
  - Handlungen
  - Mitarbeiter
  - …

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Einbusse bei Knowhow

Durch eine temporäre Race-Condition im TCP/IP-Stack konnte ein Integer-Overflow erzwungen werden. Die darauf folgende Speicherschutz verletzung hat den Heap partiell überschrieben und zum totalen Ausfall der neuen tokenbasierten Authentisierung geführt. Sorry.

- Interne Mitarbeiter kennen technische Hintergründe nicht mehr
- Externer (Cloud-)Partner hat Wissensvorsprung
- Verhandlungen und Diskussionen werden schwieriger
- Probleme können nicht mehr selber angegangen werden
  - Abhängigkeit
  - Trägheit

Intro
Wer?
Was?
Risiken
Transparenz
Vermengung
Kontrolle
Backup/Restore
Abhängigkeit
Migration
Jur. Konflikte
Verantwortung
Knowhow
Zentralisierung
Abschluss
Zusammenfassung
Fragen

Risiken | Zentraler Angriffspunkt

- Die Cloud an sich ist grundlegender Single Point of Failure (SPOF)
- Die Cloud wird zentrale Anlaufstelle für Angriffe
- Vertrauensbeziehungen innerhalb der Cloud sind gefährlich

Intro
- Wer?
- Was?

Risiken
- Transparenz
- Vermengung
- Kontrolle
- Backup/Restore
- Abhängigkeit
- Migration
- Jur. Konflikte
- Verantwortung
- Knowhow
- Zentralisierung

Abschluss
- Zusammenfassung
- Fragen

Zusammenfassung

- Cloud Computing ist ein neuer Name für ein altes Konzept (Outsourcing, Grid Computing, ASP, …)
- Es handelt sich um einen marketing-getriebenen Hype (Beginn ca. Q1-2008)
- Es gibt verschiedene Ansätze und Produkte des Cloud Computing (SaaS, PaaS, IaaS, …)
- Eine wohlüberlegte Migration kann durchaus Vorteile erlangen lassen
- Aber eine Vielzahl an sicherheitstechnischen Überlegungen sprechen gegen Outsourcing, Virtualisierung und Cloud Computing

Intro
- Wer?
- Was?

Risiken
- Transparenz
- Vermengung
- Kontrolle
- Backup/Restore
- Abhängigkeit
- Migration
- Jur. Konflikte
- Verantwortung
- Knowhow
- Zentralisierung

Abschluss
- Zusammenfassung
- Fragen

Literatur

- Die Sicherheit von Cloud Computing, http://www.scip.ch/?labs.20111110
- 10 sicherheitsrelevante Gründe gegen Cloud Computing, http://www.scip.ch/?labs.20091127

Intro
- Wer?
- Was?

Risiken
- Transparenz
- Vermengung
- Kontrolle
- Backup/Restore
- Abhängigkeit
- Migration
- Jur. Konflikte
- Verantwortung
- Knowhow
- Zentralisierung

Abschluss
- Zusammenfassung
- Fragen

Fragen

Intro
- Wer?
- Was?

Risiken
- Transparenz
- Vermengung
- Kontrolle
- Backup/Restore
- Abhängigkeit
- Migration
- Jur. Konflikte
- Verantwortung
- Knowhow
- Zentralisierung

Abschluss
- Zusammenfassung
- Fragen

Security is our Business!

scip AG
Badenerstrasse 551
CH-8048 Zürich

Tel +41 44 404 13 13
Fax +41 44 404 13 14
Mail info@scip.ch
Web http://www.scip.ch
Twitter http://twitter.com/scipag

)SCIP(

☑ Strategy | Consulting
☑ Auditing | Testing
☑ Forensics | Analysis