Mechanismen der IT-Sicherheit zum Schutz geistigen Eigentums

Michael Herfert
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Darmstadt

„ Investition in Ihre Zukunft "
HESSEN
Investitionen für diese Entwicklung wurden von der Europäischen Union aus dem Europäischen Fonds für regionale Entwicklung und vom Land Hessen kofinanziert

CIRECS - Center for Industrial Research in Cloud Security

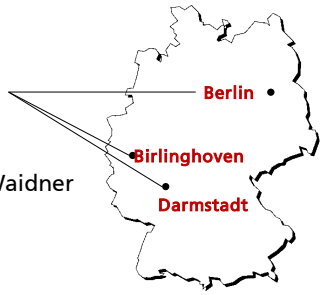
Inhalt

1. Cloud Computing
2. Angriffe auf Daten
3. Verschlüsselung von Daten in der Cloud
4. Zukunft
5. Zusammenfassung

Fraunhofer-Institut für Sichere Informationstechnologie

Fraunhofer SIT Darmstadt

Gegründet: 1961
Leitung: Prof. Dr. Michael Waidner



Fraunhofer SIT Darmstadt

170 Mitarbeiter

TECHNISCHE UNIVERSITÄT DARMSTADT

2 Lehrstühle
Prof. Sadeghi
Prof. Waidner

HESSEN

CASED

BMBF ECSPRIDE

Spin-offs:

cosee seeking your content

facilityboss GmbH

MobileSitter

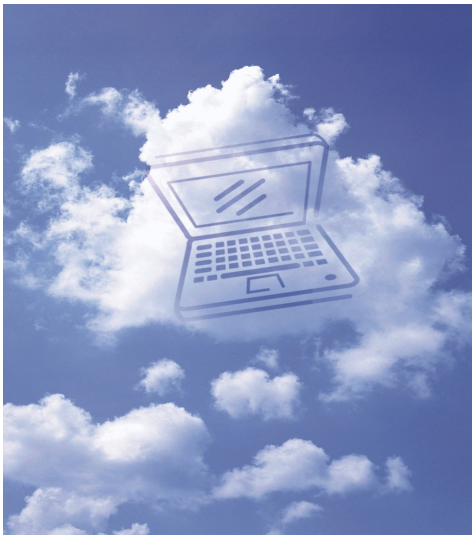
Inhalt

1. Cloud Computing
2. Angriffe auf Daten
3. Verschlüsselung von Daten in der Cloud
4. Zukunft
5. Zusammenfassung

Eigene Server = eigener Aufwand

- **Eigene Server erfordern:**
  - **Kosten bei Anschaffung und Aktualisierung**
  - **Pflege der Software**
  - **Sichere, klimatisierte Räume**
  - **Sicherheitsmechanismen**
  - **Einbruchserkennung**
  - **Firewall**
  - **Backup-Konzepte**
  - **Maßnahmen zur Ausfallsicherheit**
- **All das wird für den Anwender durch die Nutzung einer Cloud einfacher.**

Cloud-Computing = Auslagern von Hard- und Software in die Cloud



Neuer Wein in alten Schläuchen?

Mt 9, 17

NIST – Definition (1): Charakteristika

1. Selbstbedienung bei Bedarf
2. Netzwerkzugang
3. Ressourcenbündelung
4. Schnelle Anpassbarkeit
5. Messbarkeit

NIST – Definition (2): Service-Modelle

- Software als Service
- Plattform als Service
- Infrastruktur als Service

Inhalt

1. Cloud Computing
2. Angriffe auf Daten
3. Verschlüsselung von Daten in der Cloud
4. Zukunft
5. Zusammenfassung

Angriff auf lokale Daten

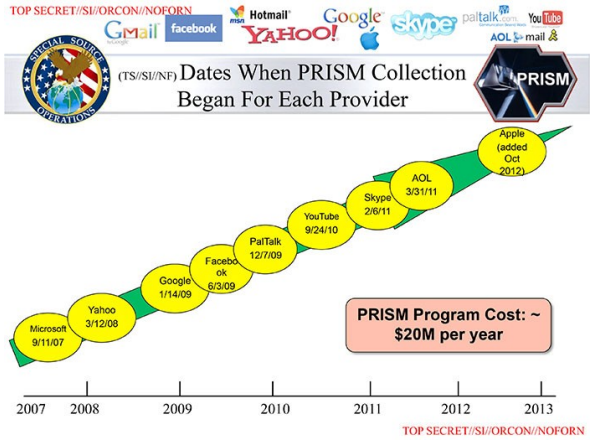
- Angriffe
  - Angriffe auf das Netzwerk
  - Viren, Würmer
  - Innentäter
  - …
- Abhilfe
  - Firewall
  - Virenscanner
  - Organisatorische Anweisungen
  - …

Angriffe auf Daten während des Transport

- Daten
  - sind während des Transports gefährdet
  - sind gefährdet, wenn sie in einer Cloud liegen
- Metadaten (IP-Adresse, to:, from:)
  - sind lesbar, selbst wenn Nachricht verschlüsselt ist
  - sind schwieriger zu verbergen

Quelle: Washington Post

Angriffe auf entfernt liegende Daten mit Unterstützung von Unternehmen



- US-Unternehmen sind verpflichtet, Daten herauszugeben
- Abhilfe:
  - Wahl von US-Unternehmen überprüfen
  - Daten verschlüsseln

Quelle: Washington Post

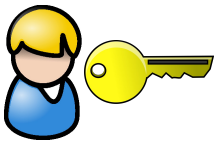
Inhalt

1. Cloud Computing
2. Angriffe auf Daten
3. Verschlüsselung von Daten in der Cloud
4. Zukunft
5. Zusammenfassung

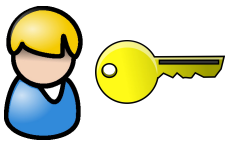
Verschlüsseln mit Hilfe der Cloud-Anbieter

1. Serverseitige Verschlüsselung

2. Verwalteter Schlüssel



3. Clientseitige Verschlüsselung

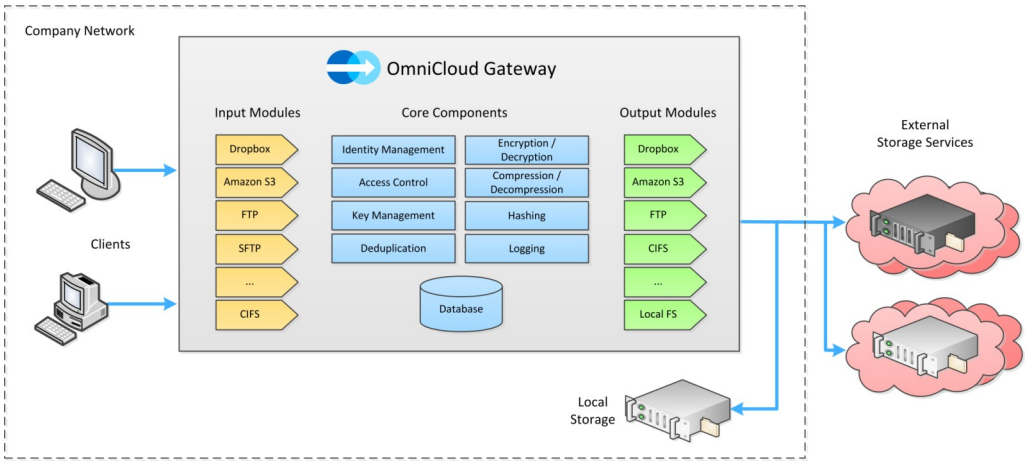


Mozy bietet auch Typ3-Verschlüsselung an

Inhalt

1. Cloud Computing
2. Angriffe auf Daten
3. Verschlüsselung von Daten in der Cloud
4. Zukunft
5. Zusammenfassung

Zukunft: OmniCloud



OmniCloud

- ist ein Server im Intranet der Firma
- wird wie ein Netzlaufwerk eingebunden
- Verschlüsselt alle Daten bevor sie in die Cloud geschickt werden

Inhalt

1. Cloud Computing
2. Angriffe auf Daten
3. Verschlüsselung von Daten in der Cloud
4. Zukunft
5. Zusammenfassung

Zusammenfassung

- Daten sind im eigenen Netz und in der Cloud gefährdet
- SSL/TLS schützt die Daten während des Transports.
  SSL/TLS ist sicher; erzwungene Eingriffsmöglichkeiten unklar
- Über SSL/TLS hinausgehende Verschlüsselung ist empfehlenswert.
  Einfach und automatisch ist besser als schwierig und händisch.
- Einige Cloud-Anbieter haben eine eingebaute Verschlüsselungsfunktionalität
  Vorsicht vor Buzz-Words („military grade encryption“)
- Computing Clouds (z.B. HR-Systeme) müssen (noch) auf Klartexten arbeiten

Kontakt

Michael Herfert
Abteilungsleiter Cloud,
Identity & Privacy

Fraunhofer-Institut für Sichere
Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Tel. 06151 869 282
Michael.Herfert@sit.fraunhofer.de