T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2014
Berlin, 03. - 04.11.2014

Bewertung von Cloud-Angeboten

Tobias Hahn
Fraunhofer Institut für sichere Informationstechnologie (SIT)

Vorstellung – Tobias Hahn

- Wissenschaftlicher Mitarbeiter im Bereich Cloud Computing, Identity und Privacy (CIP) am Fraunhofer SIT in Darmstadt
- Cloud Storage seit 2011, Forschung & Industrieprojekte
- Veröffentlichungen im Bereich Cloud Storage Sicherheit
  - „On the Security of Cloud Storage Services“, 2012
  - „Vulnerabilities through Usability Pitfalls in Cloud Services”, 2012

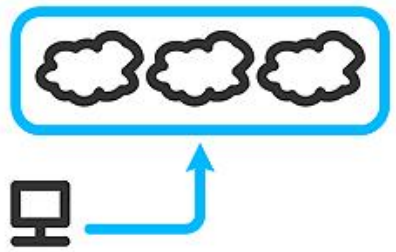
Cloud Computing

- Nutzung von Speicher / Rechenkapazität / Software bei Bedarf
- Theoretisch unbegrenzte Ressourcen verfügbar
- Infrastructure / Platform / Software as a Service
  (IaaS / PaaS / SaaS)

- Thema heute: Sicherheit von Cloud Storage Diensten
- Cloud Storage Produkte verfügbar für Endkunden, Firmen, und als Backend Lösung

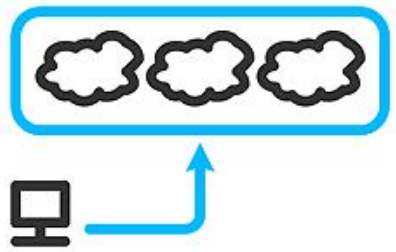
Cloud Storage

- Ablage von Daten in „der Cloud“
- Dropbox, Google Drive, iCloud, Microsoft OneDrive, …
- Vorteile:
  - Zusätzlicher Speicherplatz
  - Verfügbarkeit auf mehreren eigenen Geräten, einfaches Sharing mit anderen Nutzern
  - Schutz vor Ausfällen



Cloud Storage

- Ablage von Daten in „der Cloud“
- Dropbox, Google Drive, iCloud, Microsoft OneDrive, …
- Vorteile:
  - Zusätzlicher Speicherplatz
  - Verfügbarkeit auf mehreren eigenen Geräten, einfaches Sharing mit anderen Nutzern
  - Schutz vor Ausfällen



- Nachteile:
  - Daten werden irgendwo hin übertragen, keine Kontrolle oder Überprüfung möglich
  - Zusätzliche Angriffsmöglichkeiten

Cloud Storage – Sicher oder unsicher?

- Absolut sicher generell nicht möglich (auch nicht mit „AES256“!)

Man-in-the-Middle-Angriffe auf iCloud in China: Apple gibt Verhaltenstipps

Mac & i 22.10.2014 16

Momentan soll Berichten zufolge eine große Passwort-Abgreif-Aktion auf iCloud-Zugänge im Reich der Mitte laufen – offenbar auf Providerebene. Apple hat nun Hinweise publiziert, wie sich diese erkennen lassen.

http://www.heise.de/mac-and-i/meldung/Man-in-the-M...

Cloud Storage – Sicher oder unsicher?

- Absolut sicher generell nicht möglich (auch nicht mit „AES256“!)
- Cloud Storage nicht nur Ziel von Angriffen

Cloud Storage – Sicher oder unsicher?

- Absolut sicher generell nicht möglich (auch nicht mit „AES256“!)
- Cloud Storage nicht nur Ziel von Angriffen
- Angriffe an verschiedenen Stellen möglich

Cloud Storage – Sicher oder unsicher?

- Absolut sicher generell nicht möglich (auch nicht mit „AES256“!)
- Cloud Storage nicht nur Ziel von Angriffen
- Angriffe an verschiedenen Stellen möglich
- Attraktives Angriffsziel -> Zugriff auf persönliche Daten

Cloud Storage – Sicher oder unsicher?

- Absolut sicher generell nicht möglich (auch nicht mit „AES256“!)
- Cloud Storage nicht nur Ziel von Angriffen
- Angriffe an verschiedenen Stellen möglich
- Attraktives Angriffsziel -> Zugriff auf persönliche Daten
- Verknüpfung mit Cloud nicht immer offensichtlich

Angriffsmöglichkeiten

- Übernahme des Accounts
  - Phishing, Malware, Bruteforce
- Abhören / Verändern der Daten bei der Übertragung
- Zugriff auf die gespeicherten Daten beim Provider
  - Insider, Hacker, Geheimdienste
- Meta-Daten: Nutzung des Dienstes, Verbindungen zwischen Personen

Phase 1 – Registrierung und Login

- Email-Adresse als Nutzername
  - Verhinderung von Information Gathering möglich
- Anmeldung muss über die angegebene Email-Adresse bestätigt werden
  - Ansonsten Nutzung von Accounts im Namen anderer möglich
- Sicherheit des Login kann über Mehr-Faktor Authentifizierung erhöht werden

Phase 2 - Datenübertragung

- Unverschlüsselte Datenübertragung
  - Abhören und Modifizieren der Daten möglich
- Übertragung sollte immer TLS verwenden
  - Idealerweise sollte auch Perfect Forward Secrecy unterstützt werden
- Auch SSL/TLS angreifbar
  - MITM Angriffe sind möglich -> Zertifikats Überprüfung im CS Client
  - Schwache / gebrochene Chiffren (RC4)
  - POODLE, BEAST, Heartbeat, …

Phase 3 - Datenablage

- Unverschlüsselte Datenablage:
  - Zugriff für Provider, Geheimdienste, Insider, bei Diebstahl
- Verschlüsselte Datenablage auf dem Server
  - Oft keine genauen Infos über die Verschlüsselung
  - Provider kennt den Schlüssel -> Kann auf die Daten zugreifen
- Verschlüsselung der Daten auf dem Client
  - Ermöglicht Provider-unabhängige Sicherheit

Cloud Storage mit Client-Side Encryption

- Anbieter: SpiderOak, TeamDrive, TresorIt, …
- Schlüssel werden auf dem Client erzeugt und nur dort gespeichert
- Architektur: Häufig Hybrid-Verschlüsselung
- Vorteile
  - Sicherheit vom Provider unabhängig (wenn man der Software vertraut)

Cloud Storage mit Client-Side Encryption

- Anbieter: SpiderOak, TeamDrive, TresorIt, …
- Schlüssel werden auf dem Client erzeugt und nur dort gespeichert
- Architektur: Häufig Hybrid-Verschlüsselung
- Vorteile
  - Sicherheit vom Provider unabhängig (wenn man der Software vertraut)
- Nachteile
  - Eingeschränkter Zugriff, kein Web-Interface
  - Teurer als normale Dienste
    (~Faktor 10, Dropbox 10$/Monat 1TB, SpiderOak 10$/Monat 100GB)

Cloud Storage mit Client-Side Encryption

- Sharing mit anderen Nutzern
  - Vertrauensmodell für Schlüssel
- CSE im Browser mittels JavaScript
  - Evaluierung des Codes nicht einfach möglich
  - megapwn -> Auslesen von Schlüssel für den CSE Cloud Storage Dienst MEGA

Tobias Hahn
tobias.hahn@sit.fraunhofer.de
PGP-Key ID: 0x50610A4A