Oliver Schmitz, B. Sc.
Prof. Dr. Claus Brell

Hochschule Niederrhein
University of Applied Sciences
Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Untersuchungen der Sicherheitsaspekte von kommerziellen Cloud-Services zur Datenspeicherung im Vergleich mit dem Open Source System ownCloud für den Einsatz in KMU

Fragestellung:

- Welche Sicherheitsrisiken sind bei der Nutzung von Public Cloud Diensten wie Dropbox, SkyDrive, Google Drive und Telekom Mediencenter zu erwarten?
- Welche Sicherheitsrisiken sind im Vergleich bei einem Private Cloud Dienst mit dem Open Source System ownCloud zu beachten?
- Welche Variante ist für KMU empfehlenswert, wenn Datenverfügbarkeit als Schutzziel hohe Priorität hat?

Vergleich:

Kriterien:

- Der Vergleich zur Sicherheit von Cloud Diensten wurde für die Sicherheitsaspekte in der Tabelle durchgeführt.
- Datenschutz ist in Europa verlässlicher als in den USA. Dort können Behörden, legitimiert durch den „Patriot Act“ und den „Foreign Intelligence Surveillance Act“, vereinfacht auf Daten zugreifen, die auf US-Servern liegen.
- Für Server in Deutschland gilt das umfassendere Bundesdatenschutzgesetz (BDSG). Im europäischen Wirtschaftsraum (EWR) gelten vergleichbare Kriterien wie in Deutschland.

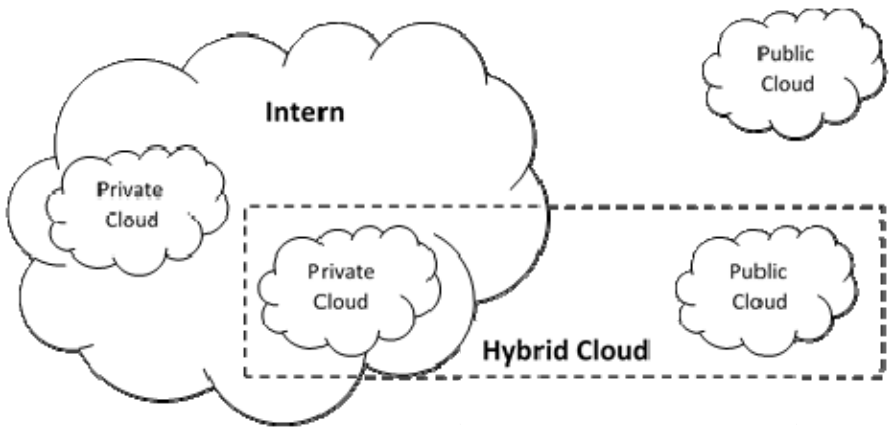
ownCloud:

- Die Performance von ownCloud ist auch beim zeitgleichen Zugriff von mehreren Clients ausreichend – auch beim Betrieb auf eine Linux-Kleinstrechner wie dem Raspberry Pi.
- Bei großer Dateianzahl zeigt der ownCloud Desktop Client sporadisch Instabilität.
- Die Verschlüsselung der Verbindung muss durch ein (eigenes) TLS (SSL) Zertifikat nachgerüstet werden.
- Seit Version 4 von ownCloud vom Mai 2012 werden die Daten auf Serverseite verschlüsselt.
- Nach entsprechender Sicherheitskonfiguration kann ownCloud auf einem Inhouse-Server über das Internet verwendet werden.

Kommerzielle Cloud Anbieter:

- Drei von vier Anbieter können keine Server im EWR garantieren und obliegen damit nicht dem strengen deutschen und europäischen Recht.
- Möchte der Nutzer wenig sensible Daten ohne großen Aufwand in der Cloud speichern, eignen sich alle vorgestellten Public Cloud Anbieter.
- Verschlüsselt der Anbieter die Daten, so kann er zur Herausgabe des Schlüssels, z.B. von Behörden, veranlasst werden.

Sicherheitsaspekt	own-Cloud	Dropbox	Telekom Medien-center	Google Drive	SkyDrive
Anbieter					
Sitz des Anbieters	nicht relevant	USA	Deutsch-land	USA	USA
Server im EWR	nicht relevant	-	✓	-	-
Datensicherung					
Datensicherung durch den Anbieter	nicht relevant	✓	✓	✓	✓
Allgemeine Geschäftsbedingungen					
Besonderheiten in den AGBs	nicht relevant	keine	keine	keine mehr	keine
Verschlüsselung der Verbindung					
Verschlüsselung der Verbindung möglich (standardmäßig)	✓ (-)	✓ (✓)	✓ (✓)	Keine Angabe	✓ (✓)
Verwendung etablierter Verschlüsselungsprotokolle möglich	✓	✓	✓	Keine Angabe	✓
Zugang zur Webseite verschlüsselt (standardmäßig)	✓ (-)	✓ (✓)	✓ (✓)	✓ (✓)	✓ (✓)
Verschlüsselung der Daten					
Verschlüsselung der Daten durch den Anbieter auf Serverseite (standardmäßig)	✓ (-)	✓ (✓)	- (-)	✓ (✓)	- (-)
Verschlüsselung der Daten durch Nutzer möglich	-	✓	✓	✓	✓
Login					
Zweistufiger Login bzw. 2-Faktor-Authentifizierung	-	✓	-	✓	✓

Handlungsempfehlungen für KMU:

- Cloud Dienste können zur Datenspeicherung und Datensicherung für KMU grundsätzlich empfohlen werden.
- Bei der Nutzung kommerzieller Cloud Dienste sollten Unternehmen für sensible Daten eine separate, client-seitige Verschlüsselung einsetzen.
- Für sensible Daten bietet sich alternativ der Betrieb einer Private Cloud mit ownCloud an.
- ownCloud kann als Private Cloud mit geringem Aufwand, kostengünstig und skalierbarem Sicherheitsniveau eingesetzt werden.
- Hohe Sicherheit, besonders hinsichtlich der Verfügbarkeit, kann durch Hybride Konzepte erreicht werden.