Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

ÜBER DIE SICHERHEIT VON CLOUD-SPEICHERDIENSTEN

MANAGEMENT SUMMARY

ÜBER DIE SICHERHEIT VON CLOUD-SPEICHERDIENSTEN

Die wachsende Menge von wertvollen digitalen Daten zu Hause und im Geschäftsumfeld muss geschützt werden, weil ein unwiederbringlicher Verlust nicht hinnehmbar ist. Cloud-Speicherdienste versprechen eine Lösung für dieses Problem, und dementsprechend hat ihre Popularität in den vergangenen Jahren stark zugenommen. Sie bieten eine benutzerfreundliche, leicht zugängliche und kostengünstige Möglichkeit, um Daten zu speichern sowie zwischen unterschiedlichen Nutzern und Endgeräten zu synchronisieren.

Privatpersonen und Unternehmen zögern jedoch damit, ihre Daten einem Cloud-Speicherdienst anzuvertrauen, weil sie befürchten, die Kontrolle über ihre Daten zu verlieren. Erfolgreiche Angriffe auf Cloud-Speicherdienste haben in jüngster Zeit diese Bedenken noch größer werden lassen. Die Dienstanbieter versuchen derweil, die Situation zu verbessern und haben Maßnahmen ergriffen, um die Daten ihrer Kunden zu schützen.

Diese Studie des Fraunhofer-Instituts für Sichere Informationstechnologie untersucht die Sicherheitsmechanismen von sieben Cloud-Speicherdiensten: CloudMe, CrashPlan, Dropbox, Mozy, TeamDrive, Ubuntu One und Wuala.

Tabelle 1 **Funktionen der Cloud-Speicherdienste**

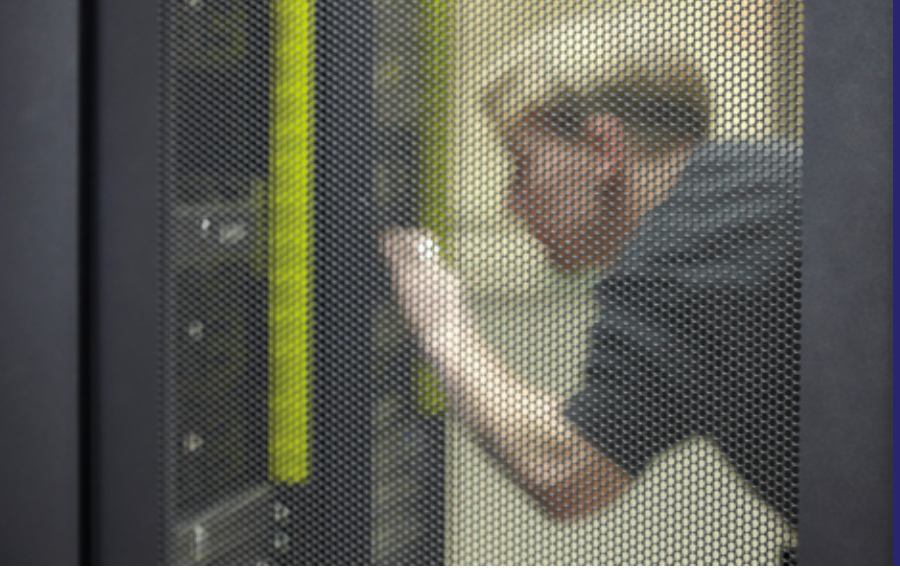
	Kopieren	Backup	Sync.	Teilen
CloudMe	✓			✓
CrashPlan		✓		
Dropbox	✓		✓	✓
Mozy		✓		
TeamDrive	✓	✓	✓	✓
Ubuntu One	✓		✓	✓
Wuala	✓	✓	✓	✓

Die Studie ist nicht nur für Nutzer der getesteten Anbieter hilfreich, sondern auch für Personen oder Unternehmen, die mithilfe der entwickelten Kriterien die Sicherheit anderer Cloud-Speicherdienste einschätzen möchten.

Herangehensweise Jeder Dienst besteht aus zwei Software-Bestandteilen, einer Client-Software für den eigenen PC sowie einer Software auf der Server-Seite. Die Testergebnisse basieren auf der Analyse der Client-Software, Penetrationstests auf Server-Seite fanden hingegen nicht statt. Die Untersuchung startete im Sommer 2011 und dauerte bis Januar 2012.

In einem ersten Schritt wurden vier typische Funktionalitäten von Cloud-Speicherdiensten identifiziert: (i) die Kopierfunktion, mit der Dienste Teile der lokalen Festplatte einfach in der Cloud spiegeln. Bei Verlust der lokalen Hardware (z. B. bei Diebstahl eines Laptops) lassen sich die Daten aus der Cloud heraus wiederherstellen. (ii) Die Backup-Funktion, die dazu dient, jede Version einer Datei in der Cloud zu speichern. (iii) Die Synchronisationsfunktion, die Nutzer in die Lage versetzt, Dateien auf verschiedenen Geräten zu synchronisieren (Desktop-PC, Laptop, Tablet, Smartphone, etc.). (iv) Die Filesharing-Funktion, die oft in Kooperationen mit Projektpartnern eingesetzt wird. Jeder Dienst besitzt eine oder mehrere der beschriebenen Funktionen (siehe Tabelle 1). Zusätzlich haben die Forscher Funktionen identifiziert, welche die Nutzung der Grundfunktionen optimieren können. Hierzu zählt etwa die Deduplikations-Funktion (Daten, die bereits auf dem Cloud-Server existieren, werden nicht erneut hochgeladen).

Im zweiten Schritt wurden Sicherheitsanforderungen aufgestellt. Die fünf wichtigsten Anforderungen und Zielsetzungen sind: (i) Registrierung und Anmeldung, um starke Passwörter sicherzustellen und damit die Herausgabe unnötiger persön-



licher Daten zu verhindern, um vor dem Unterschieben von belastenden Daten zu schützen. (ii) Transportsicherheit zum Schutz der Kommunikation zwischen Server und Client-PC. (iii) Verschlüsselung, um Daten vor dem Zugriff der Dienstanbieter zu schützen. (iv) Sicheres Filesharing, um Dokumente zu schützen, die innerhalb einer geschlossenen Gruppe geteilt werden, optional auch mit Zugang für Nicht-Kunden des Dienstes. (v) Sichere Deduplikation, um Datenschutzprobleme zu vermeiden, die bei der Deduplikation entstehen können.

Ergebnisse Die Anwendung der Sicherheitsanforderungen auf die ausgewählten Dienste führte zu den in Tabelle II dargestellten Ergebnissen.

Registrierung war ein Problem für CloudMe, Dropbox und Wuala, weil diese Anbieter keine Bestätigungs-E-Mail an ihre Nutzer versenden. Dadurch ist es möglich, illegales Material hochzuladen, das einem anderen Nutzer angelastet wird. Dazu registriert sich eine Person A mit einer fremden E-Mail-Adresse der Person B. Anschließend kann Nutzer A illegales Material hochladen und dann die Polizei auf die illegalen Inhalte aufmerksam machen, die B zugeschrieben werden.

Transportsicherheit war ein Problem für CrashPlan, TeamDrive und Wuala, denn sie verwenden nicht das etablierte SSL/TLS-Protokoll. Stattdessen verwenden sie unveröffentlichte proprietäre Protokolle – ein erfahrungsgemäß sehr fehleranfälliger Ansatz. CloudMe hat keinerlei Maßnahmen ergriffen, um die Daten während des Transports zu schützen.

Verschlüsselungsprobleme fanden die Tester bei CloudMe, Dropbox und Ubuntu One, denn diese Dienste bieten keine Verschlüsselung auf Client-Seite. Dadurch kann der Dienstanbieter die Daten einsehen. Mozy verschlüsselt Daten, aber keine Dateinamen. Das besondere Verschlüsselungsverfahren von Wuala ermöglicht Angriffe von Server-Seite.

Teilen von Daten / Filesharing war ein Problem für CloudMe, Dropbox, TeamDrive und Wuala. Mangelhaft bewertet wurde, wenn Dateien unter Verwendung mangelhaft verschleierter In-

Tabelle 2 **Bewertung**

	Registrierung	Transport	Verschlüsselung	Teilen	Deduplikation
CloudMe	– –	– –	– –	–	x
CrashPlan	+	+ –	+	x	+
Dropbox	–	+	–	+ –	+
Mozy	+ –	+	+ –	x	–
TeamDrive	+ –	+ –	+	+ –	x
Ubuntu One	++	+	– –	++	+
Wuala	–	+ –	+ –	+ –	–

++	sehr gut
+	gut
+ –	einige Schwächen
–	schlecht
– –	sehr schlecht
x	nicht abrufbar

ternet-Adressen mit Personen geteilt werden konnten, die nicht Nutzer des jeweiligen Cloud-Dienstes waren. CloudMe weist hier Mängel auf. Dropbox macht keine klaren Aussagen darüber, wer genau Zugriff auf die fraglichen Dateien hat. TeamDrive besitzt Schwächen, wenn es darum geht, Gruppenmitglieder auszuladen, und Wuala ermöglicht unerwünschte Datensammlungen, weil Nutzernamen Teil der öffentlich zugänglichen Internet-Adresse sind. Die fraglichen Arbeitsbereiche von CloudMe lassen sich von Suchmaschinen durchsuchen.

Deduplikation war ein Problem für Mozy und Wuala, denn in manchen Fällen lässt sich durch eine Anfrage prüfen, ob eine Datei bereits in der Cloud existiert. Die Vertraulichkeit von Daten kann verbessert werden, wenn Nutzer ihre Daten lokal verschlüsseln, bevor sie diese in die Cloud hochladen. Dazu kann man Verschlüsselungswerkzeuge wie TrueCrypt, EncFS oder GnuPrivacyGuard nutzen. Mitunter lassen sich bei Verwendung solcher Werkzeuge aber nicht mehr alle Funktionen der Cloud-Speicherdienste nutzen. Nutzer sollten sich zudem bewusst sein, dass sie ihre Daten dem Provider anvertrauen, wenn sie dessen Client-Software benutzen. Eine fehlerhafte Client-Software kann großen Schaden erzeugen.

Rechtliche Überlegungen Zusätzlich betrachtet die Studie auch rechtliche Anforderungen hinsichtlich einer gesetzeskonformen Nutzung von Cloud-Speicherdiensten. Eine Prüfung der Gesetze und der rechtlichen Vorgaben ergab, dass in erster Linie der Cloud-Nutzer die Verantwortung für seine Daten und deren Verarbeitung trägt. Besonders Unternehmen müssen deshalb die rechtlichen Anforderungen beachten und sich bewusst sein, dass der Cloud-Anbieter möglicherweise anderen Anforderungen unterworfen ist. Da es keine internationalen Regelungen gibt, die genügend Datensicherheit und Datenschutz gewährleisten, sollten Unternehmen aus der EU einen Cloud-Anbieter wählen, der im europäischen Wirtschaftsraum beheimatet ist und nicht zu einem Unternehmen aus den USA gehört. Andernfalls können amerikanische Regierungsbehörden auf Grundlage des Patriot Act Zugang zu den gespeicherten Daten erhalten – selbst wenn diese ausschließlich in Europa gespeichert sind.

Zusammenfassung Einzelpersonen oder Unternehmen, die überlegen, einen Cloud-Speicherdienst zu nutzen, sollten prüfen, ob die fraglichen Anbieter die beschriebenen Sicherheitsanforderungen erfüllen. Zusätzlich kann es ratsam sein, mehr als einen Dienst zu nutzen, um die Auswirkungen von Fehlzeiten zu reduzieren. Des Weiteren empfiehlt es sich auch, die Zeit zu berechnen, die für die Wiederherstellung aller Daten zu veranschlagen ist. Abhängig von der jeweiligen Datenmenge kann dies einige Tage in Anspruch nehmen. Wer sich einen Anbieterwechsel offen lassen will, ist gut beraten, vorsorglich einen entsprechenden Plan auszuarbeiten, das verringert die eigene Abhängigkeit von einem bestimmten Anbieter (provider lock-in). Ein Wechsel kann beispielsweise notwendig werden, wenn ein Anbieter zu teuer wird oder nicht mehr den gesetzlichen Anforderungen entspricht.

Ein wesentliches Ergebnis der Studie ist, dass alle Provider sich der großen Bedeutung von Datensicherheit und Datenschutz bewusst sind und Schutzmaßnahmen ergriffen haben. Dennoch konnte unter den betrachteten Anbietern keine Lösung gefunden werden, die alle zugrundeliegenden Sicherheitsanforderungen erfüllt.

Kostenfreier Download
Die komplette Studie kann heruntergeladen werden unter **http://sit4.me/cloudstudy2012**

Kontakt
Michael Herfert
Telefon 06151 869-329
Fax 06151 869-322
michael.herfert@sit.fraunhofer.de

Fraunhofer-Institut für Sichere Informationtechnologie
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de