Whitepaper

OmniCloud – Sichere und flexible Nutzung von Cloud-Speicherdiensten

Thomas Kunz, Ruben Wolf

Fraunhofer-Institut für Sichere
Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt

2014

„Investition in Ihre Zukunft“

Investitionen für diese Entwicklung wurden von der Europäischen Union aus dem Europäischen Fonds für regionale Entwicklung und vom Land Hessen kofinanziert

Inhaltsverzeichnis

Zusammenfassung **3**

1. Einleitung **4**
1.1. Datenspeicherung in der Cloud 5
1.2. Sicherheit von Cloud-Speicherangeboten 5

2. OmniCloud **6**
2.1. Anwendungsszenarien 7
2.2. OmniCloud-Features im Überblick 8

3. Technischer Überblick **10**
3.1. Enterprise-Gateway-Ansatz 10
3.2. Design-Prinzipien 11
3.3. Architekturkomponenten 12
3.4. Cloud-Schnittstellen und Speicherstrategien 14

4. Datensicherheit **15**
4.1. Sicherheitsannahmen 16
4.2. Authentifizierung 17
4.3. Zugriffskontrolle 19
4.4. Lokale Dateiverschlüsselung und Schlüsselmanagement 19
4.5. Verschleierung von Datei- und Verzeichnisnamen 21
4.6. Weitere Aspekte von Datensicherheit 21

5. Vermeidung von Dopplungen durch Deduplikation **22**

6. Leichter Anbieterwechsel durch Umzugsdienst **24**

Literatur **26**

A. Häufig gestellte Fragen (FAQ) **28**

Über Fraunhofer SIT **33**

Zusammenfassung

Viele Unternehmen haben trotz der Vorteile, die Cloud-Dienste bieten, große Bedenken, ihre Geschäftsdaten einem Cloud-Speicherdienst anzuvertrauen. Fraunhofer SIT stellt mit OmniCloud eine Lösung bereit, mit deren Hilfe Unternehmen Cloud-Speicherdienste sicher nutzen können. Die grundlegende Idee von OmniCloud ist, beliebige Anwendungs- und Backup-Software mit beliebigen Cloud-Speicherdiensten zu verbinden. OmniCloud gewährleistet die Vertraulichkeit der gespeicherten Daten – unabhängig von den konkreten Sicherheitsmechanismen oder aktuellen Sicherheitsvorfällen beim Cloud-Anbieter. Mit OmniCloud werden Unternehmen in die Lage versetzt, Cloud-Speicherangebote in sicherer Weise zu nutzen und somit Kosten bei der Sicherung ihrer digitalen Daten einzusparen. Des Weiteren unterstützt OmniCloud Unternehmen auf effiziente Weise beim Wechsel des Cloud-Anbieters und beugt so einer ungewünschten Bindung an einen Anbieter vor.

1. Einleitung

Die Popularität von Cloud-Speicherdiensten ist in den vergangenen Jahren sehr stark angestiegen. Dienste wie Dropbox verfügen über mehr als 100 Millionen registrierte Nutzer, die täglich mehr als 1 Milliarde Dateien speichern (Stand: November 2012)[Cons12]. Für Unternehmen sind Cloud-Speicherdienste sehr attraktiv für die externe Datenspeicherung und für Datensicherungen. Neben einem professionellen Management und physischer Sicherheit der gespeicherten Daten, ist der verfügbare Cloud-Speicherplatz nahezu unbegrenzt und extrem kostengünstig.

Die Nutzung von Cloud-Speicherdiensten birgt jedoch auch Risiken, insbesondere hinsichtlich der Sicherheit und Vertraulichkeit der gespeicherten Daten. Auch Bedenken hinsichtlich der Verfügbarkeit und des Kontrollverlusts über die Daten werden diskutiert. Die Nutzung von Cloud-Speicherdiensten setzt das Vertrauen in den Cloud-Anbieter voraus. Zu den internen Sicherheitspolitiken kommen weitere Service-Level-Agreements (SLA) der Cloud-Anbieter hinzu. Zudem ist häufig nicht leicht festzustellen, wo und von wem die Daten tatsächlich verarbeitet und gespeichert werden. Cloud-Anbieter nutzen teilweise andere Cloud-Anbieter als Unterauftragnehmer (Dropbox nutzt z. B. den Amazon S3-Dienst). Dies kann dazu führen, dass Nutzer und Cloud-Anbieter unterschiedlichen rechtlichen Bestimmungen unterliegen, Compliance-Anforderungen u. U. nicht erfüllbar oder Daten nicht mehr vor staatlichem Zugriff geschützt sind (vgl. „Patriot-Act“).

Des Weiteren ist derzeit der Markt an Cloud-Speicherdiensten noch sehr heterogen. Neue Dienste und attraktivere Angebote entstehen und weniger erfolgreiche Dienste verschwinden. Für Unternehmen ist hierbei einerseits wichtig, nicht dauerhaft an einen Cloud-Dienst gebunden zu sein („Provider-Lock-In“) und andererseits (etwa im Falle einer Insolvenz des derzeitigen Cloud-Anbieters) leicht zu einem anderen Cloud-Anbieter wechseln zu können.

Das Fraunhofer SIT hat mit OmniCloud eine Lösung konzipiert, welche die besonderen Aspekte der Cloud-Speichernutzung in Unternehmen berücksichtigt und die Nutzung von Cloud-Speicherdiensten für Unternehmen sicher und flexibel gestaltet. OmniCloud verschlüsselt alle Dateien lokal bevor sie das Unternehmensnetzwerk verlassen und zum Cloud-Speicher transferiert werden. So bleiben die Unternehmensdaten vertraulich, unabhängig davon, welche Sicherheitsmechanismen der genutzte Cloud-Speicheranbieter bereitstellt. Konkrete Sicherheitsvorfälle beim Cloud-Speicheranbieter haben durch die Nutzung von OmniCloud keine Auswirkungen und keine Durchschlagskraft auf die Vertraulichkeit der gespeicherten Unternehmensdaten. Gleichzeitig unterstützt OmniCloud das Unternehmen aktiv beim Cloud-Anbieterwechsel. Mittels des OmniCloud-Umzugsdienstes werden die Daten effizient von dem alten zum neuen Cloud-Anbieter verschoben.

OmniCloud liegt derzeit als Konzept vor. Einige Funktionen wurden bereits prototypisch realisiert und bei verschiedenen Veranstaltungen vorgestellt. Wegen des großen Erfolgs und den vielen positiven Rückmeldungen potenzieller Anwender plant Fraunhofer SIT, OmniCloud zu einem real verwert- und vermarktbaren Produkt weiter zu entwickeln. Hierzu sucht Fraunhofer SIT derzeit geeignete Partner aus der Wirtschaft für die Entwicklung und den Vertrieb von OmniCloud.

1.1. Datenspeicherung in der Cloud

Bereits heute existieren viele wertvolle Informationen in Unternehmen, wie beispielsweise Verträge oder Geschäftspläne, nur noch in digitaler Form, und dieser Trend wird sich in Zukunft noch weiter verstärken. Diese Daten müssen geschützt werden, denn ein unwiderruflicher Verlust kann im schlimmsten Fall den Ruin eines Unternehmens bedeuten. Zudem sind Unternehmen rechtlich verpflichtet, bestimmte Daten wie etwa Steuerunterlagen über längere Zeit aufzubewahren.

Aus diesen Gründen erstellen nahezu alle Unternehmen Backups ihrer Daten. Das korrekte Erstellen von Backups ist jedoch aufwändig: Backups müssen physikalisch und räumlich getrennt von den Originaldaten aufbewahrt werden, da ansonsten im Falle eines Diebstahls oder Feuerschadens sowohl die Originaldaten, als auch die Backups betroffen sein können. Zudem erfordern regelmäßig erzeugte Backups einen hohen Speicherplatz. Große Unternehmen sind in der Lage, sich zu diesem Zweck dedizierte Datencenter („Private Cloud“) aufzubauen. Für kleinere und mittlere Unternehmen (KMU) kommt dies häufig aus finanziellen Gründen nicht in Frage. Insbesondere für diese Unternehmen bietet sich mit Cloud-Computing eine Lösung für diese Probleme. Spezielle Cloud-Speicherdienste versprechen nahezu unbegrenzte Speicherkapazitäten zu sehr günstigen Preisen. Die Zahl der Anbieter solcher Cloud-Speicherdienste ist sehr groß. Die Datencenter dieser Anbieter werden professionell betrieben, sind physikalisch gegen Diebstahl und Feuerschäden geschützt und sind mit Hardware ausgestattet, die für einen Betrieb rund um die Uhr ausgelegt ist, einschließlich unterbrechungsfreier Stromversorgung, um auch gegen Stromausfälle geschützt zu sein.

Die Verwendung von Cloud-Speicherdiensten als Backup-Medium scheint somit eine ideale Lösung zu sein, die hilft Kosten zu reduzieren und zudem die Verfügbarkeit der Daten erhöht. Trotzdem zögern viele Unternehmen damit, ihre Daten der Cloud anzuvertrauen. Sie fürchten, dass der Schutz ihrer Daten nicht ausreichend gesichert ist: Sowohl der Cloud-Anbieter selbst als auch Angreifer könnten in den Besitz vertraulicher Daten kommen. Zudem sind die Daten nicht vor dem Zugriff durch Regierungen geschützt („US Patriot Act“). Hinzu kommen rechtliche Bedenken, wenn Daten einem anderen Unternehmen (Cloud-Anbieter) anvertraut werden. Des Weiteren befürchten Unternehmen, an einen bestimmten Cloud-Anbieter gebunden zu sein, da ein Wechsel des Anbieters oft nur schwer möglich ist („Provider Lock-in“).

1.2. Sicherheit von Cloud-Speicherangeboten

Viele Unternehmen haben trotz der Vorteile, die Cloud-Dienste bieten, große Bedenken, ihre Geschäftsdaten einem Cloud-Speicherdienst anzuvertrauen. Viele Sicherheitsaspekte, wie Datenschutz, Datenintegrität und Verfügbarkeit müssen sorgfältig betrachtet werden. Zu dem selben Schluss kommen viele unabhängige Studien. Ein Sicherheitsreport der Deutschen Telekom aus dem Jahr 2011[Deut11] befragte Entscheidungsträger aus Unternehmen über die Bedeutung von IT-Sicherheit. Sie kamen zu dem Schluss,

dass IT-Sicherheit eine sehr hohe (67%) oder zumindest hohe (29%) Signifikanz hat. Eine Studie von CapGemini kam zu dem Ergebnis, dass der Einsatz von Public-Cloud-Diensten nicht stark steigen wird, solange die damit verbundenen Sicherheitsprobleme nicht gelöst sind [Capg12]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) identifizierte ein zusätzliches Hindernis bei der Verwendung von Cloud-Diensten: Der Verlust von Kontrolle und der direkten Einflussnahme hinsichtlich der Umsetzung von Sicherheitsmechanismen[BSI12].

Das Fraunhofer-Institut für Sichere Informationstechnologie SIT hat im März 2012 im Rahmen einer Studie[BHHK+12] das Thema Sicherheit von Cloud-Speicherdiensten näher untersucht. In dieser Studie wurde die Sicherheit von sieben Cloud-Speicherdiensten, die sich primär an Privatkunden richten, analysiert. Die Studie zeigte, dass sich die Anbieter solcher Cloud-Speicherdienste zwar der Bedeutung von IT-Sicherheit bewusst sind, trotzdem aber keiner der getesteten Dienste auch nur die notwendigsten Sicherheitsanforderungen erfüllte. Typische Mängel, die aufgedeckt wurden, sind

- eine fehlende lokale Verschlüsselung der Daten,
- Probleme bei der Freigabe von Dateien für andere Personen, durch die es auch unberechtigten Personen möglich ist, auf die eigenen Daten zuzugreifen,
- eine fehlende Verifikation der E-Mail-Adresse bei der Registrierung, die es Angreifern ermöglicht, sich unter einer falschen Identität bei einem Dienst zu registrieren und es ihnen dann erlaubt, ihren Opfern beispielsweise Schadsoftware unterzuschieben oder Datenspionage zu betreiben,
- Schwächen bei der Registrierung und Anmeldung, durch die es u. a. möglich ist, schwache Passwörter für die Anmeldung zu wählen oder E-Mail-Adressen bereits registrierter Nutzer auszuspähen.

2. OmniCloud

Fraunhofer SIT stellt mit OmniCloud eine Lösung bereit, mit deren Hilfe Unternehmen Cloud-Speicherdienste sicher nutzen können. Die grundlegende Idee von OmniCloud ist, beliebige Anwendungs- und Backup-Software mit beliebigen Cloud-Speicherdiensten zu verbinden. Hierbei erfolgt die Speicherung derart, dass die Vertraulichkeit der Daten geschützt wird, unabhängig von den konkreten Sicherheitsmechanismen beim Cloud-Anbieter. Fraunhofer SIT reagiert damit auf die oben genannten Bedenken hinsichtlich der Nutzung von Cloud-Speichern und die Anforderungen von insbesondere kleinen und mittleren Unternehmen bezüglich sicherem Cloud-Speicher. Mit OmniCloud werden Unternehmen in die Lage versetzt, Cloud-Speicherangebote in sicherer Weise zu nutzen und somit Kosten bei der Sicherung ihrer digitalen Daten einzusparen.

Ziele und Nutzen

1. **OmniCloud macht Cloud-Speicher sicherer.** OmniCloud verschlüsselt alle Dateien lokal im Unternehmensnetzwerk bevor sie in die Cloud übertragen werden. Für jede Datei wird ein separater Verschlüsselungsschlüssel verwendet. Zusätzlich zu den eigentlichen Dateiinhalten werden auch alle Dateinamen und Verzeichnisstrukturen verschleiert. Vor dem Zugriff auf OmniCloud werden die Benutzer authentifiziert. Mit Hilfe eines Zugriffskontrollmechanismus kann feingranular festgelegt werden, welche Benutzer auf welche Dateien zugreifen können.

2. **OmniCloud macht Software cloud-fähig.** OmniCloud dient als Adapter, mit dem beliebige Anwendungs- und Backup-Software cloud-fähig gemacht werden kann. OmniCloud stellt hierfür eine Reihe von verbreiteten Standard-Kommunikationsschnittstellen zur Verfügung, die von allen gängigen Betriebssystemen und Software-Produkten unterstützt werden. Eine Installation von OmniCloud auf den einzelnen Endgeräten ist hierfür nicht notwendig. Stattdessen stellt sich OmniCloud seinen Benutzern ähnlich wie ein Netzlaufwerk oder ein FTP-Server dar, das zum Speichern entweder direkt genutzt oder zunächst mit einem Laufwerksbuchstaben verbunden werden kann.

3. **OmniCloud verhindert die Bindung an einen Cloud-Anbieter.** OmniCloud verhindert die Abhängigkeit von einem bestimmten Cloud-Speicheranbieter. Normalerweise ist ein Umzug der gespeicherten Daten eine große Hürde für Unternehmen. Mit OmniCloud können die Daten bei Bedarf einfach und schnell zu einem neuen Cloud-Speicherdienst verlagert werden. OmniCloud unterstützt die Verlagerung aktiv durch einen eigenen Umzugsdienst. Die Daten müssen hierzu weder in das Unternehmensnetzwerk heruntergeladen noch neu verschlüsselt werden.

Typische Anwender von OmniCloud

OmniCloud wurde für den Unternehmenseinsatz entwickelt und richtet sich insbesondere an kleine und mittlere Unternehmen, welche die Vorteile von Cloud-Speichern nutzen möchten, andererseits aber auch hohe Anforderungen an die Sicherheit der gespeicherten Daten stellen. OmniCloud ist gerade auch für solche Unternehmen interessant, die über kein Budget für die Einrichtung einer Private-Cloud-Lösung verfügen. Mit OmniCloud lassen sich auch Public-Cloud-Lösungen sicher verwenden.

2.1. Anwendungsszenarien

Durch einen modularen Aufbau lassen sich mit OmniCloud eine Vielzahl von Anwendungsszenarien realisieren. Die konkrete Funktionalität ergibt sich hierbei durch die Auswahl und Konfiguration der einzelnen OmniCloud-Funktionsbausteine. So bietet OmniCloud Unternehmen ein hohes Maß an Sicherheit und gleichzeitig große Flexibilität.

Nachfolgend sind einige Anwendungsszenarien von OmniCloud exemplarisch dargestellt. Viele weitere Szenarien sind möglich.

Redundantes Daten-Backup in der Cloud und lokal. OmniCloud erlaubt die Anbindung mehrerer Cloud-Speicherdienste und lokaler Speicher. Auf diese Weise lässt sich ein redundanter Speicher für die Nutzung bei Daten-Backups erreichen. Die Daten werden dann mehrfach, bei verschiedenen Anbietern (und zusätzlich auch lokal im Unternehmensnetzwerk) verschlüsselt gespeichert.

Kombination mehrerer Cloud-Speicher zu einem großen. OmniCloud ist in der Lage, verschiedene Cloud-Speicherangebote zu kombinieren. So können Nutzer vorhandene Angebote (wie solche von DropBox und ähnlichen Anbietern) zusammenschließen und diese als ein großes Laufwerk in die eigene Unternehmensumgebung einbinden. OmniCloud prüft hierbei den Füllstand der einzelnen Angebote. Sobald ein Cloud-Speicher voll ist, nutzt OmniCloud ein anderes Angebot.

Datenaustausch über einen gemeinsamen Projektordner. Mit OmniCloud können Unternehmen Ordner für Abteilungen oder Projektgruppen einrichten, die von Mitarbeitern für den Austausch von Dateien genutzt werden. Aus Benutzersicht verhält sich OmniCloud hierbei wie ein Netzwerklaufwerk.

Dynamische Teams und Änderungen von Zuständigkeiten. Im Gegensatz zu vielen anderen Verschlüsselungslösungen eignet sich OmniCloud für dynamische Teams und berücksichtigt typische Unternehmenssituationen wie Mitarbeiterausfälle und Änderungen von Zuständigkeiten.

2.2. OmniCloud-Features im Überblick

OmniCloud bietet eine Fülle von Funktionen und Eigenschaften, um die Nutzung von Cloud-Speicherdiensten sicher und flexibel zu gestalten. Nachfolgend werden die wesentlichen Features im Überblick dargestellt.

Die **Datenverschlüsselung** ist die wichtigste Funktion von OmniCloud. OmniCloud verschlüsselt alle Dateien bevor sie das Unternehmensnetzwerk verlassen. Die zur Verschlüsselung verwendeten Schlüssel werden im Unternehmensnetzwerk generiert und sind dem Anbieter des Cloud-Speicherdienstes nicht bekannt. Mit Hilfe von zusätzlichen Sicherheitsmechanismen wie **Authentifizierung und Zugriffskontrolle** kann genau festgelegt werden, welche Benutzer auf welche Dateien innerhalb von OmniCloud zugreifen können.

OmniCloud erlaubt eine **einfache Integration** in die existierende Systeminfrastruktur innerhalb des Unternehmensnetzwerks. Hierfür ist **keine Installation** einer OmniCloud-Software auf den Endgeräten der Benutzer notwendig. OmniCloud unterstützt verschiedene **Standard-Kommunikationsprotokolle**, die von vielen Betriebssystemen und Applikationen direkt unterstützt werden.

OmniCloud unterstützt eine **Vielzahl von Cloud-Speicherdiensten**, wie Amazon S3, Dropbox oder Box. Neue Dienste können leicht integriert werden.

OmniCloud kann **Cloud-Speicherplatz einsparen** und so die **Cloud-Speicherkosten reduzieren**. In einem Unternehmen werden die gleichen Daten oft an mehreren Stellen gespeichert. OmniCloud erkennt solche Dopplungen und sorgt dafür, dass jeweils nur ein Exemplar im Cloud-Speicher landet (Deduplikation).

Mit Hilfe von **Speicherstrategien** kann festgelegt werden, wie OmniCloud die eingehenden Daten auf die konfigurierten Cloud-Speicherdienste verteilt. OmniCloud übernimmt hierbei die Anpassung bzw. Übersetzung zwischen den verschiedenen Cloud-Schnittstellen. Mittels einer Speicherstrategie kann beispielsweise festgelegt werden, dass die verschlüsselten Daten in mehreren Cloud-Speicherdiensten und lokalen Datenspeichern abgelegt werden sollen („Mirroring“), um die **Redundanz** zu erhöhen. OmniCloud erlaubt auch die Bildung eines großen Cloud-Speichers durch Kombination mehrerer kleiner Cloud-Speicher. OmniCloud überwacht hierbei die Füllstände der Cloud-Speicher und verteilt die eingehenden Daten entsprechend („Striping“). Weitere Speicherstrategien können einfach integriert werden.

OmniCloud bietet einen **Umzugsdienst** für die im Cloud-Speicher gespeicherten Daten. Dieser Umzugsdienst kann die ungewünschte Bindung an den Anbieter eines Cloud-Speicherdienstes („Provider Lock-in“) verhindern. Der Umzugsdienst selbst läuft in der Cloud und kann daher von den schnellen Netzwerk-Datenübertragungsraten profitieren. Das Herunterladen und eine Neuverschlüsselung der Daten sind nicht notwendig.

Das OmniCloud zugrunde liegende **Vertrauensmodell** trennt streng zwischen dem lokalen Unternehmensnetzwerk, in dem OmniCloud läuft, und der Cloud-Anbieterseite. Zur Verdeutlichung der Wichtigkeit dieser Eigenschaft könnte man sich Cloud-Speicherdienste (wie beispielsweise Crashplan oder Mozy) vorstellen, die ebenfalls lokale Verschlüsselung anbieten. Auf der einen Seite erfordern diese Dienste nicht, dass ein Benutzer dem Dienstanbieter vertraut, da alle Dateien lokal verschlüsselt werden, bevor sie den Computer des Benutzers verlassen. Auf der anderen Seite stellen diese Anbieter gleichzeitig ihren Benutzern die Software zur Verfügung, die auf den Endgeräten der Benutzer installiert werden muss, und welche die Schlüsselgenerierung und Verschlüsselung übernimmt. Das diesen Lösungen zugrundeliegende Vertrauensmodell ist problematisch. Auch wenn man nicht davon ausgehen kann, dass irgendein Cloud-Anbieter unlautere Absichten verfolgt, so existieren aber dennoch Möglichkeiten, dass sich die Client-Software nicht wie gewünscht verhält, beispielsweise aufgrund eines Software-Fehlers. Des Weiteren sind Cloud-Speicheranbieter als Aggregator großer Mengen von Daten attraktive Angriffsziele für Spionage und Infiltration.

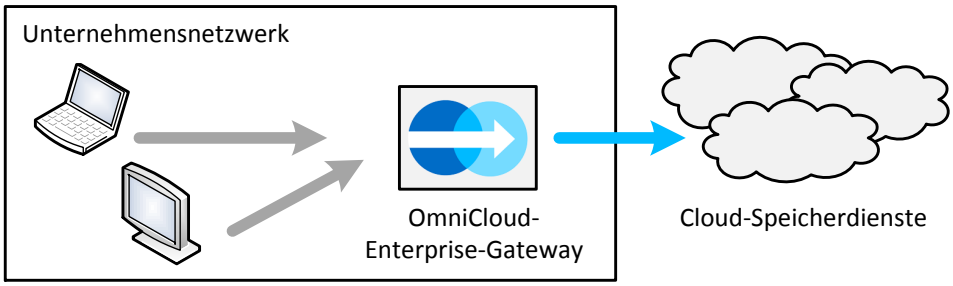

Abbildung 1: OmniCloud als Enterprise-Gateway

3. Technischer Überblick

3.1. Enterprise-Gateway-Ansatz

OmniCloud wurde derart konzipiert, dass es innerhalb eines Unternehmensnetzwerks läuft. Hierbei arbeitet OmniCloud als sogenanntes Enterprise-Gateway in Form einer Netzwerk-Appliance oder eines Servers, wie in Abbildung 1 dargestellt. Durch Nutzung des OmniCloud-Gateway erhalten alle Mitarbeiter sicheren Zugriff auf die von OmniCloud genutzten Cloud-Speicherdienste. OmniCloud übernimmt hierbei für den Benutzer unsichtbar die Umsetzung der Sicherheitsmechanismen (wie beispielsweise die Verschlüsselung der Daten). Mittels Standard-Software (beispielsweise Dateimanager oder Backup-Programmen) können sich Benutzer mit OmniCloud verbinden und Daten kopieren oder austauschen. Eine Installation einer dedizierten OmniCloud-Applikation auf den Endgeräten der Benutzer ist hierfür nicht notwendig.

OmniCloud unterstützt typische Interaktionsmuster und Anwendungsfälle wie beispielsweise die Speicherung von Datenkopien in der Cloud, das Erzeugen von Backups in der Cloud oder das direkte Arbeiten auf den entfernt gespeicherten Dateien. Im Rahmen von OmniCloud bedeutet der Begriff „unterstützt“ hierbei, dass der Benutzer eine entsprechende Software (beispielsweise eine Backup-Software) nutzt, die Standard-Speicherschnittstellen, wie beispielsweise FTP[PoRe85], Amazon S3[Amaz] oder Secure Copy (SCP)[Orac], bietet. Die folgenden Speicherfunktionen bietet OmniCloud:

Kopieren. Die Kopier-Funktion erzeugt *ad-hoc* eine *exakte Kopie* der aktuellen lokalen Daten in der Cloud. Ein typischer Benutzer möchte auf diese Weise sicherstellen, dass die Daten auch dann noch verfügbar sind, wenn die lokale Hardware ausfällt (beispielsweise durch Schaden oder Diebstahl). Hierbei ist anzumerken, dass OmniCloud für die Ver- und Entschlüsselung der Daten verantwortlich ist, d. h. auf die Kopien der Daten in der Cloud kann nur über OmniCloud zugegriffen. Der Zugriff von außerhalb des Unternehmensnetzwerks (beispielsweise von einem Internet-Café oder beim Kunden) ist i. A. nur über eine VPN-Verbindung zum OmniCloud-Gateway bzw. durch Portfreischaltung der Unternehmens-Firewall für einzelne OmniCloud-Dienste möglich.

Datensicherung. Die Backup-Funktion erlaubt die Wiederherstellung einer *beliebigen Version* der zuvor gespeicherten Dateien oder Verzeichnisse über einen langen Zeitraum hinweg. Die Erstellung von Backups in der Cloud ist i. d. R. ein automatisierter Prozess, der *regelmäßig* Kopien der Daten anfertigt und diese Daten in einen Cloud-Speicher transportiert, damit diese im Schadensfall wiederhergestellt werden können.

Netzwerklaufwerk. Diese Funktion erlaubt es, OmniCloud wie ein Netzwerklaufwerk einzusetzen. Benutzer können somit direkt auf den entfernt gespeicherten Daten arbeiten, indem Sie entweder geeignete Software und Kommunikationsprotokolle (wie beispielsweise FTP oder WebDAV[Duss07]) nutzen oder OmniCloud als Netzwerkspeicher im Betriebssystem verbinden.

3.2. Design-Prinzipien

Einfache Integration. OmniCloud soll sich einfach in bestehende IT-Infrastrukturen integrieren lassen. Zu diesem Zweck unterstützt OmniCloud unterschiedliche Kommunikationsprotokolle (z. B. FTP, WebDAV, verschiedene Cloud-Schnittstellen wie Amazon S3), sodass viele Client-Applikationen (z. B. Backup- oder FTP-Software) zusammen mit OmniCloud verwendet werden können, um Dateien in der Cloud zu speichern. Dies bedeutet, dass OmniCloud keinen dedizierten OmniCloud-Client benötigt, der auf den Rechnern der Anwender installiert werden muss. Zudem unterstützt OmniCloud eine Vielzahl an Cloud-Speicherdiensten und ermöglicht es den Anwendern somit, einen geeigneten Cloud-Speicherdienst auszuwählen.

Trennung von Dateien und Schlüsseln. OmniCloud speichert ausschließlich verschlüsselte Dateien in der Cloud. Die Schlüssel, die für die Ver- und Entschlüsselung der Dateien verwendet werden, verbleiben im eigenen Unternehmen und werden von OmniCloud selbst verwaltet. Auf diese Weise ist es für die Cloud-Speicherdienste unmöglich, die Dateien zu entschlüsseln.

Trennung von Meta-Informationen und Schlüsseln. OmniCloud speichert Meta-Informationen über die Dateien (z. B. Dateinamen, Eigentümer der Dateien, Speicherort der Dateien in der Cloud) in einer lokalen Datenbank. Die Schlüssel, die für die Ver- und Entschlüsselung benötigt werden, werden ebenfalls lokal gespeichert, allerdings getrennt von den Meta-Informationen. Stattdessen verwendet OmniCloud einen sicheren Schlüsselmanager für die Speicherung der Schlüssel. Durch diese Maßnahme wird verhindert, dass nicht-autorisierte Insider Zugriff auf die Schlüssel erlangen.

Selbst-Replikation. Eine installierte OmniCloud-Instanz kann im Falle eines schweren Fehlers (z. B. nach einem Festplatten-Crash) jederzeit wiederhergestellt werden. Zu diesem Zweck werden alle Daten, die OmniCloud in der lokalen Datenbank verwaltet sowie sämtliche Konfigurationsdateien in einen Backup-Prozess integriert. Dieser

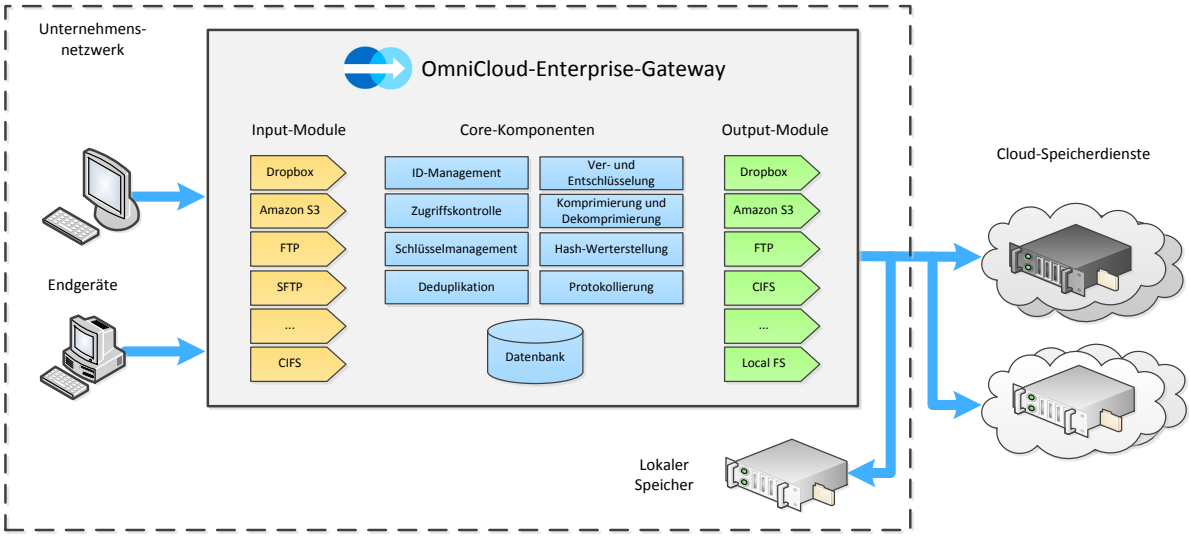

Abbildung 2: OmniCloud-Komponenten

Backup-Prozess verschlüsselt in periodischen Abständen diese Daten mit einem dedizierten Master-Schlüssel und speichert die auf diese Weise verschlüsselten Daten an geeigneter Stelle. Der für die Speicherung dieser OmniCloud-Backups verwendete Cloud-Speicherdienst muss nicht notwendigerweise der gleiche sein, der auch für die Speicherung der verschlüsselten Anwenderdateien genutzt wird.

Im Falle eines Datenverlusts ist der Administrator von OmniCloud in der Lage, diese OmniCloud-Backups herunterzuladen und die OmniCloud-Installation mithilfe des aufbewahrten Master-Schlüssels wiederherzustellen.

Gemeinsame Ressourcen. OmniCloud kann dazu genutzt werden, verschiedenen Nutzern Zugriff auf die gleichen in der Cloud gespeicherten Ressourcen zu gewähren. Das bedeutet, dass OmniCloud diesen Nutzern eine gemeinsame Sicht auf die gemeinsam genutzten Ressourcen zur Verfügung stellt. Hierbei werden alle Operationen auf diesen Dateien transparent im Hintergrund synchronisiert. Zusätzlich kann auf diese Ressourcen simultan über unterschiedliche Protokolle zugegriffen werden (z. B. FTP und CIFS[HeLP96]).

3.3. Architekturkomponenten

Dieser Abschnitt gibt einen Überblick über die grundlegenden Architekturkomponenten von OmniCloud (vgl. Abbildung 2). Die Komponenten sind in sogenannte Input-Module (gelb), Output-Module (grün) und Core-Komponenten (blau) gruppiert. Auf der linken Seite befinden sich die Clients der Anwender, die über das Unternehmensnetzwerk auf das OmniCloud-Gateway zugreifen.

Datensenken. OmniCloud kann mehrere externe Cloud-Speicherdienste (rechte Seite in Abbildung 2) verwenden, um beispielsweise die Dateien der Anwender auf mehreren Cloud-Speicherdiensten zu spiegeln. Außerdem kann OmniCloud die Dateien zusätzlich auf lokalen Laufwerken innerhalb des Unternehmensnetzwerks speichern, um auf diese Weise die Verfügbarkeit der Dateien im Falle von Internet-Problemen zu erhöhen. Interne und externe Speicher werden im Folgenden zusammenfassend als Datensenken bezeichnet.

Input-Module. Die Input-Module sind für die Authentifizierung der Nutzer verantwortlich, nehmen die Anfragen der Clients entgegen und leiten diese an die Core-Komponenten weiter. Jedes Input-Modul unterstützt ein bestimmtes Kommunikationsprotokoll (z. B. FTP oder Amazon S3). OmniCloud kann mehrere Input-Module parallel betreiben, um auf diese Weise unterschiedliche Kommunikationsprotokolle anzubieten.

Output-Module. Die Output-Module sind für die Kommunikation mit den Datensenken verantwortlich. Sie nehmen die Anfragen von den Core-Komponenten entgegen und bilden sie auf dienstspezifische Anfragen ab. Genau wie die Input-Module unterstützt jedes Output-Modul genau eine Datensenke (z. B. durch die Verwendung einer REST-Schnittstelle[Fiel00]). Durch die simultane Verwendung mehrerer Output-Module wird eine redundante Speicherung in unterschiedlichen Datensenken ermöglicht.

Sowohl die Input- als auch die Output-Module sind als leichtgewichtige Komponenten mit geringer Funktionalität konzipiert. Dadurch wird die Implementierung zusätzlicher Module extrem vereinfacht. Für anspruchsvollere Funktionalitäten, wie z. B. die Authentifizierung der Nutzer, können die Input- und Output-Module auf entsprechende Core-Komponenten zurückgreifen.

Core-Komponenten. Die Core-Komponenten verarbeiten die Nutzeranfragen. Jede Core-Komponente ist für eine spezielle Aufgabe verantwortlich, wie beispielsweise das Identitätsmanagement (IDM), das Schlüsselmanagement, die Ver- und Entschlüsselung der Dateien sowie die Bildung von Hash-Werten der Dateien.

OmniCloud-Dienste. OmniCloud-Dienste stellen ein Konzept dar, um Input- und Output-Module, Datensenken und unterschiedliche Konfigurationen zu gruppieren. D. h., aus technischer Sicht ist ein OmniCloud-Dienst eine Zusammenstellung bestehend aus einer Menge von Input-Modulen, einer Menge von Output-Modulen, einer Menge unterstützter Operationen[1] sowie einer konkreten OmniCloud-Konfiguration.

Damit stellen OmniCloud-Dienste einen sehr flexiblen Weg dar, unterschiedliche Funktionalitäten bereitzustellen. OmniCloud kann eine beliebige Anzahl von Diensten definieren, wobei jeder Dienst über eine eigene Konfiguration und damit über eine andere Funktionalität verfügt. Beispielsweise könnte ein Dienst jede Datei verschlüsseln, weil die Dateien bei einem externen Cloud-Speicherdienst gespeichert werden, ein anderer Dienst

[1] Unter einer *Operation* wird eine Dateisystemoperation verstanden, welche die Client-Anwendung des Benutzers aufruft (z. B. „Speichere eine Datei bei einem Cloud-Dienst“, „Lade eine Datei von einem Cloud-Dienst“, „Lösche eine Datei“ usw.).

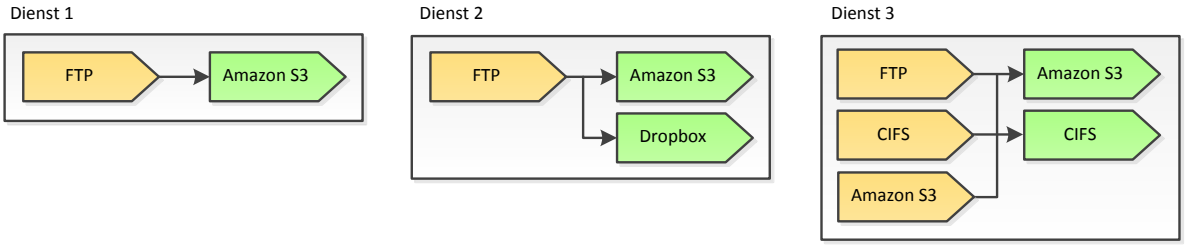

Abbildung 3: Übersetzung zwischen Kommunikationsprotokollen

könnte jedoch darauf verzichten, da er die Dateien lediglich lokal speichert. Weiterhin kann jedem OmniCloud-Dienst eine eigene Menge autorisierter Nutzer zugeordnet werden[2]. Abhängig von der jeweiligen Sicherheitspolitik eines Dienstes können Nutzer eines Dienstes autorisiert sein, auf Dateien anderer Nutzer dieses Dienstes zuzugreifen. Prinzipiell können die dazu nötigen Zugriffsregeln in beliebiger Granularität definiert werden. Dadurch ermöglicht das Konzept der OmniCloud-Dienste die Definition gemeinsam genutzter Ressourcen.

3.4. Cloud-Schnittstellen und Speicherstrategien

Anbindung von Cloud-Schnittstellen

Ein wichtiges Konzept von OmniCloud ist die Möglichkeit, verschiedene Input-Module, über die Benutzer mit OmniCloud kommunizieren, mit verschiedenen Output-Modulen, mit deren Hilfe die Daten in der Cloud gespeichert werden, zu verbinden („API-Mapping“). OmniCloud übernimmt hierbei die Übersetzung zwischen den Schnittstellen und Kommunikationsprotokollen der Input- und Output-Module. Für jeden einzelnen OmniCloud-Dienst kann hierbei festgelegt werden, welche Input- und Output-Module miteinander verbunden werden sollen. Hierbei sind nicht nur einfache *1-zu-1*-Beziehungen zwischen Input- und Output-Modulen möglich, sondern auch komplexere Gebilde, wie beispielsweise *1-zu-n*-, *m-zu-1*- oder *m-zu-n*-Beziehungen (siehe Abbildung 3).

Die Übersetzung zwischen verschiedenen Input- und Output-Modulen hat für die Benutzer von OmniCloud den Vorteil, dass die Cloud-Speicherangebote auch dann genutzt werden können, wenn die verwendete Client-Software das vom Cloud-Anbieter angebotene Kommunikationsprotokoll nicht nativ unterstützt. OmniCloud macht Software cloud-fähig. Eine existierende Backup-Lösung, die beispielsweise nur FTP, CIFS oder SCP zur Speicherung der Daten unterstützt, kann auf diese Weise dennoch mit Cloud-Speicherdiensten wie Amazon S3 oder Dropbox genutzt werden. Des Weiteren kann der Cloud-Speicheranbieter einfach gewechselt werden, ohne dass Veränderungen in der Client-Software durchgeführt werden müssen. Die Bindung an einen bestimmten Cloud-Anbieter kann somit verhindert werden.

[2] Aber ein Nutzer kann für den Zugriff auf mehr als einen Dienst autorisiert sein.

Speicherstrategien

Bei der Speicherung von Daten in der Cloud erlaubt OmniCloud die Verwendung unterschiedlicher Speicherstrategien. Jeder OmniCloud-Dienst besitzt genau eine Speicherstrategie. Diese definiert die Art und Weise, in der OmniCloud die Dateien in den Cloud-Speichern ablegt. Als Bestandteil der Speicherstrategie wird beispielsweise festgelegt, welche Cloud-Speicherdienste verwendet werden sollen und wie die Daten zwischen diesen Cloud-Speicherdiensten verteilt werden. Die folgende Aufzählung zeigt Beispiele für Speicherstrategien:

- Speicherung aller Dateien im gleichen Cloud-Speicher,
- Speicherung der Dateien in mehreren Cloud-Speichern („Mirroring“),
- Speicherung der Dateien in mindestens m von n Cloud-Speichern,
- Speicherung aller Dateien auf einem lokalen Datenspeicher im Unternehmensnetzwerk und zusätzlich noch in einem von n Cloud-Speichern,
- Nutzung von Reed-Solomon-Kodierungsverfahren zur Erhöhung der Fehlertoleranz, wie beispielsweise in [AbPW10] vorgeschlagen wurde,
- Aufteilung der Dateien in Teilstücke unter Verwendung von Information-Dispersal-Verfahren, wie beispielsweise in [SeGS11] und [Sp$^+$ot11] vorgeschlagen wurde.

Der modulare Ansatz von OmniCloud und vorhandene Programmschnittstellen erlauben es, neue Speicherstrategien in einfacher Weise zu realisieren.

4. Datensicherheit

Bei der Nutzung von Cloud-Speicherdiensten für geschäftliche Zwecke müssen weitere Anforderungen erfüllt sein, die sich einerseits aus dem Wert der Daten für das Unternehmen selbst und andererseits aus existierenden rechtlichen Rahmenwerken (Compliance-Standards) ergeben. Diese haben auch Auswirkungen in Hinblick auf die Datensicherheit, insbesondere auf das effektive und effiziente Identitäts- und Rechte- und Schlüsselmanagement. Existierende Cloud-Speicherangebote für private Endbenutzer berücksichtigen diese Aspekte in der Regel unzureichend. OmniCloud hingegen bietet effiziente Managementfunktionen, die sich einfach in bestehende Prozesse zur Benutzer-Provisionierung integrieren lassen.

Das Hauptziel von OmniCloud ist hierbei, die Benutzung von Cloud-Speicherdiensten aus der Sicht des Benutzers sicherer zu machen. OmniCloud bietet hierfür verschiedene Sicherheitsmechanismen wie Authentifizierung der Benutzer, Zugriffskontrolle, Verschlüsselung sowie zugehörige Werkzeuge für Identitäts-, Rechte- und Schlüsselmanagement. Die wichtigsten Sicherheitsfunktionen von OmniCloud werden nachfolgend vorgestellt.

4.1. Sicherheitsannahmen

Als Grundlage und zum Verständnis der Sicherheitsmechanismen von OmniCloud werden zunächst einige Sicherheits- und Vertrauensannahmen beschrieben.

Es wird angenommen, dass OmniCloud innerhalb des Intranets eines Unternehmens als Enterprise-Gateway (vgl. Abschnitt 3.1) installiert ist. Nur autorisierte Mitarbeiter haben Zugriff auf die Dienste, die vom OmniCloud-Gateway bereitgestellt werden. Hierfür müssen sich die Mitarbeiter zunächst mittels eines unterstützten Verfahrens unter Verwendung eines zugehörigen Berechtigungsnachweises authentifizieren. Berechtigungsnachweise werden von ausgewiesenen Stellen innerhalb des Unternehmens an die Mitarbeiter ausgegeben. Weiterhin schützen Benutzer ihre Berechtigungsnachweise vor unautorisiertem Zugriff und geben diese nicht weiter. Das Unternehmen, welches das OmniCloud-Gateway betreibt, vertraut seinen Mitarbeitern, dass diese das Gateway gemäß der vorgesehenen Verwendung nutzen. Weitere zugehörige Benutzungsregeln werden sowohl technisch als auch organisatorisch umgesetzt.

OmniCloud-Dienste definieren einen abgegrenzten Bereich, in dem Dienstnutzer zusammenarbeiten können. Dienstnutzer eines bestimmten Dienstes stehen in einem besonderen Vertrauensverhältnis, wenngleich nicht alle Benutzer die gleichen Zugriffsrechte auf die verarbeiteten Dateien besitzen.

Das OmniCloud-Gateway wird von dedizierten OmniCloud-Administratoren verwaltet, von denen angenommen wird, dass sie ihrerseits ebenfalls Mitarbeiter des Unternehmens sind, welches das OmniCloud-Gateway betreibt. Diese Administratoren haben Zugriff auf die administrativen OmniCloud-Komponenten und -Schnittstellen, richten neue Benutzer ein, verteilen Berechtigungsnachweise an Benutzer, richten neue OmniCloud-Dienste ein und definieren Zugriffsrechte für Dienste. Außerdem haben sie Zugriff auf alle OmniCloud-Datenbanken und Konfigurationsdateien, die OmniCloud-relevante Meta-Informationen speichern. OmniCloud-Administratoren sind ebenfalls mit Berechtigungsnachweisen ausgestattet. Es wird angenommen, dass OmniCloud-Administratoren diese Berechtigungsnachweise in besonderer Weise vor unautorisiertem Zugriff schützen und nicht weitergeben.

Die Schlüsselmanagement-Komponente von OmniCloud erzeugt und speichert alle zur Ver- und Entschlüsselung von Dateien benötigen Schlüssel. Die Vertraulichkeit dieser Schlüssel ist durch zusätzliche Mechanismen geschützt. Beim Start des OmniCloud-Gateway muss ein OmniCloud-Administrator die notwendigen Berechtigungsnachweise

bzw. Schlüssel bereitstellen bzw. aktivieren, um die Schlüsselmanagement-Komponente zu initialisieren. Dieser Ansatz ist vergleichbar mit dem Start eines HTTPS-Webservers, bei dem der Administrator durch Eingabe einer Geheimkombination den privaten Schlüssel aktiviert. Der Berechtigungsnachweis bzw. Schlüssel ist der Vertrauensanker für die OmniCloud-Schlüsselmanagement-Komponente, ohne diesen können weder neue Dateien verschlüsselt noch existierende entschlüsselt werden. Er kann beispielsweise als kryptographischer Schlüssel oder als Smartcard mit zugehöriger PIN realisiert werden.

Es wird angenommen, dass alle Benutzer und Administratoren des OmniCloud-Gateway ihre Berechtigungsnachweise derart schützen, dass mögliche Sicherheitsvorfälle minimiert werden.Verliert ein OmniCloud-Benutzer seinen Berechtigungsnachweis, wird dieser für die weitere Verwendung gesperrt und ein neuer Berechtigungsnachweis ausgestellt. Um einen hohen Grad an Verfügbarkeit des OmniCloud-Gateway zu gewährleisten, sollten zusätzliche Maßnahmen ergriffen werden, um das gewünschte Maß an Verfügbarkeit, Zuverlässigkeit und Performanz zu erreichen. Des Weiteren sind Datensicherungen notwendig, um die OmniCloud-internen Verwaltungsinformationen zu sichern. Diese Datensicherungen müssen durch geeignete Maßnahmen vor unautorisiertem Zugriff und Veränderung geschützt werden.

In Bezug auf die Cloud-Speicheranbieter wird angenommen, dass diese sich konform zu den vereinbarten Verträgen und Dienstgütezusagen verhalten, beispielsweise hinsichtlich der Integrität und Verfügbarkeit der gespeicherten Daten. Die Vertraulichkeit der gespeicherten Daten wird jedoch (auch entgegen zugehöriger Dienstgütezusagen) nicht angenommen. Hingegen wird angenommen, dass aufgrund unterschiedlicher Ursachen wie staatliche Regularien, Datenlecks oder bösartigen Angriffen die Vertraulichkeit der Daten beeinträchtigt werden kann. Aus diesem Grund bietet OmniCloud einen Mechanismus, mit dem die gespeicherten Informationen vertraulich bleiben, selbst wenn die Dateien beim Cloud-Speicheranbieter öffentlich würden.

4.2. Authentifizierung

Die Authentifizierung von OmniCloud-Benutzern ist der grundlegende Sicherheitsmechanismus, auf dem nachfolgende Sicherheitsmechanismen aufbauen. Benutzer müssen sich gegenüber dem verwendeten Input-Modul eines OmniCloud-Dienstes authentifizieren, beispielsweise gegenüber dem FTP-Server eines OmniCloud-Dienstes. Da Benutzer u. U. Zugriff auf verschiedene OmniCloud-Dienste haben, können sie auch verschiedene Berechtigungsnachweise für verschiedene Authentifizierungsarten besitzen. Hierfür kann es unterschiedliche Authentifizierungsverfahren geben, die in den einzelnen Input-Modulen eines Dienstes zum Einsatz kommen. So unterscheidet sich beispielsweise das Authentifizierungsverfahren eines SFTP-Servers[File] von dem eines CIFS-Servers.

Input-Module wurden als leichtgewichtige Komponenten entwickelt, d. h. sie stellen unter Umständen nicht die gesamte Funktionalität hinsichtlich des ID-Managements selbst

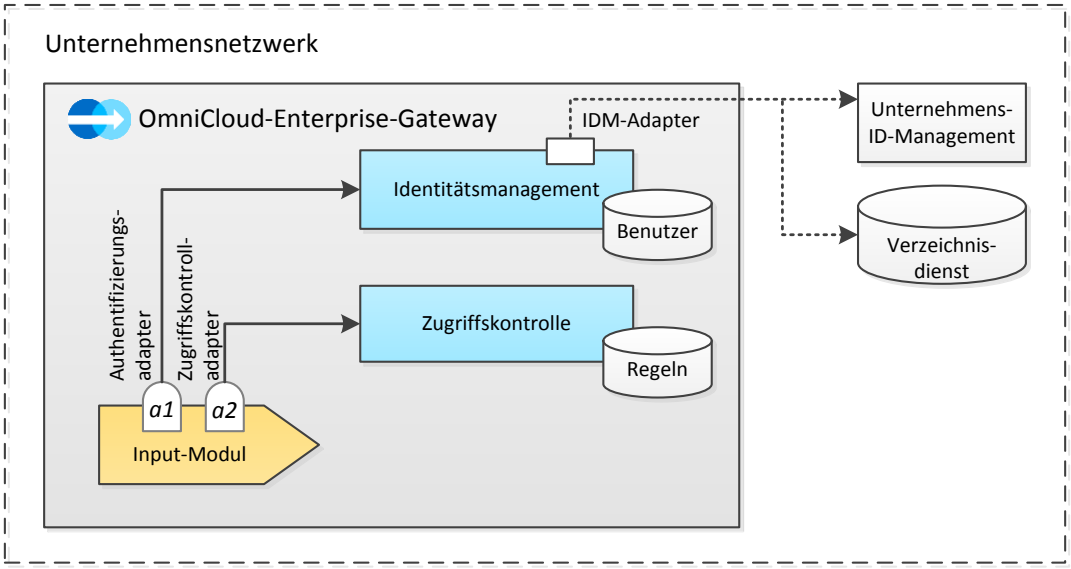

Abbildung 4: Anbindung der Identitätsmanagement- und Zugriffskontroll-Komponenten

bereit. Stattdessen können sie auf Core-Komponenten des OmniCloud-Gateway zurückgreifen, wie beispielsweise die Identitätsmanagement-Komponente, welche über alle Referenzwerte verfügt, um Berechtigungsnachweise zu prüfen. Diese Identitätsmanagement-Komponente kann mit den Berechtigungsnachweisen für die verschiedenen Authentifizierungsprotokolle umgehen (beispielsweise Passwörter, Hash-Werte von Passwörtern, öffentliche Schlüssel für Public-Key-basierte Verfahren).

Zwischen Input-Modulen und der Identitätsmanagement-Komponente besteht i. d. R. die folgende Arbeitsteilung: Input-Module realisieren das jeweilige Authentifizierungsprotokoll während die Identitätsmanagement-Komponente die gelieferten Berechtigungsnachweise überprüft. Dies wird durch entsprechende Adapter in den Input-Modulen erreicht. Abbildung 4 zeigt ein Beispiel-Input-Modul mit dem Authentifizierungsadapter *a1* zur Anbindung der Identitätsmanagement-Komponente.

Die Identitätsmanagement-Komponente ist zusätzlich dafür verantwortlich, die Input-Modul-spezifischen Identitäten auf OmniCloud-weite Identitäten abzubilden. Um die Verwaltung der OmniCloud-Identitäten zu vereinfachen, kann die Identitätsmanagement-Komponente mit der zentralen Identitätsmanagement-Komponente des Unternehmens durch einen IDM-Adapter verbunden sein (siehe Abbildung 4).

Berechtigungsnachweise für die Administration von OmniCloud werden separat von denen regulärer OmniCloud-Benutzer verwaltet. Auf die Darstellung der Details der zugrundeliegenden Mechanismen wird jedoch hier verzichtet. Neben der Authentifizierung von Benutzern findet an bestimmten Stellen auch eine Authentifizierung von OmniCloud-Komponenten untereinander statt. Zugehörige Details sind ebenfalls nicht Gegenstand dieses Dokuments.

4.3. Zugriffskontrolle

OmniCloud bietet einen Mechanismus für rollenbasierte Zugriffskontrolle. Für jeden OmniCloud-Dienst kann festgelegt werden, welche Benutzer welche Operationen auf welchen Dateien ausführen dürfen. Benutzer lassen sich zur einfachen Verwaltung von Rechten mittels Rollen gruppieren. Die Zugriffsregeln können sich von Dienst zu Dienst hinsichtlich ihres Granularitätsgrades unterscheiden, um eine dem Anwendungsszenario angemessene, kompakte Menge von Regeln zu erhalten. Zugriffsregeln können definiert werden über Benutzer, Rollenzugehörigkeiten, Verzeichnisse, Dateien oder Dateieigenschaften. Selbst komplexere Zugriffsregeln, die beispielsweise dynamische Kontextinformationen (wie Datum, Uhrzeit oder IP-Adresse) berücksichtigen, lassen sich realisieren. Hierfür können Kontextsensoren definiert werden, welche den aktuellen Kontextwert zum Zeitpunkt der Zugriffskontrollentscheidung liefern (vgl. [WoKS03, NeSt04, AlWo09]). Um die Verwaltung von Zugriffsregeln zu erleichtern und die Benutzbarkeit und Effizienz zu steigern, können sogar simultan Zugriffsregeln unterschiedlicher Granularitätsgrade definiert werden.

Die Zugriffskontrolle ist in ähnlicher Weise wie die Authentifizierung in die Input-Module integriert. Mittels eines Zugriffskontrolladapters und mit Unterstützung der Core-Komponente für die Zugriffskontrolle werden die Zugriffskontrollentscheidungen im Input-Modul durchgesetzt (siehe Abbildung 4). Die Zugriffsregeln werden mittels der ORKA-Policy-Language (OPL) [AlWP09] definiert. Die komplette Syntax und zugehörige formale Semantik wurde in [AlWo09] beschrieben.

Ausdrucksstärke. Die folgenden Zugriffsregeln sind Beispiele für die große Ausdrucksstärke der OPL-Sprache: (1) Alle Benutzer eines Dienstes haben vollen Zugriff auf alle Dateien eines Dienstes. (2) Nur Benutzer A, B und C dürfen Dateien in Verzeichnis X überschreiben. (3) Alle Benutzer dürfen die Dateien lesen, aber nur die Eigentümer dürfen ihre Dateien modifizieren. (4) Dateien mit der Dateiendung *.docx* dürfen nur dann überschrieben werden, wenn die Operation nicht an Wochenenden stattfindet und die Temperatur in Darmstadt über 20 Grad Celsius liegt.

Die Konfiguration von OmniCloud-Diensten für bestimmte Anwendungsszenarien (Projekte, Abteilungen, etc.) und die Definition von zugehörigen Zugriffsregeln ist ein wirkungsvolles Instrument, um den Zugriff auf die in Cloud-Speichern abgelegten Dateien zu kontrollieren.

4.4. Lokale Dateiverschlüsselung und Schlüsselmanagement

Wie bereits oben ausgeführt, verlässt sich OmniCloud nicht auf die Maßnahmen des Cloud-Speicheranbieters zur Sicherung der Vertraulichkeit der gespeicherten Dateien. Daher werden alle Dateien lokal auf dem OmniCloud-Gateway verschlüsselt, bevor sie extern gespeichert werden. Alle Dateien werden hierbei mit unterschiedlichen Schlüsseln

verschlüsselt. OmniCloud unterstützt verschiedene symmetrische Ver- und Entschlüsselungsalgorithmen und -modi.

Um den Sicherheitsgrad zur erhöhen, werden die Verschlüsselungsschlüssel nicht zusammen mit den zugehörigen Meta-Informationen der Dateien gespeichert. Stattdessen wird hierfür eine Schlüsselmanagement-Komponente verwendet, deren Hauptzweck ist, neue Schlüssel zu generieren, diese zusammen mit einer ID abzuspeichern und auf Anfrage oder Vorlage der ID an die Ver- bzw. Entschlüsselungskomponente auszuliefern. Die Schnittstelle der Schlüsselmanagement-Komponente ist derart entwickelt, dass es möglich ist, andere Umsetzungen (und auch dedizierte Hardware-Komponenten mit entsprechenden Programmschnittstellen) zu integrieren. So könnte beispielsweise für die Schlüsselgenerierung auf eine besonders sichere Entropie-Quelle zugegriffen werden. Die Daten der Schlüsselmanagement-Komponente sind durch spezielle Berechtigungsnachweise oder Sicherheits-Token geschützt, die beim Start des OmniCloud-Gateway zur Initialisierung vorgelegt werden müssen. Verschlüsselungsschlüssel werden weder unverschlüsselt auf dem Gateway noch zusammen mit den verschlüsselten Dateien beim Cloud-Speicheranbieter abgelegt.

Die zur Verschlüsselung verwendeten Schlüssel werden pseudo-zufällig (oder bei geeigneter Entropie-Quelle auch zufällig) erzeugt. OmniCloud setzt im Gegensatz zu anderen Cloud-Verschlüsselungslösungen keine passwortbasierte Verschlüsselung („Password-based Encryption“, „PBE“) ein. Hintergrund: Bei PBE-basierten Verfahren werden die kryptographischen Schlüssel aus Passwörtern abgeleitet. Der resultierende Schlüsselraum ist in der Praxis selbst bei großen Passwortlängen und großen Zeichenmengen im Vergleich zum Schlüsselraum des Verschlüsselungsverfahrens verschwindend klein. Daher ist es ein Trugschluss zu denken, dass kryptographische Schlüssel, die durch passwortbasierte Ableitungsfunktionen erzeugt wurden, zufällig und mit der Sicherheit zufälliger Schlüssel vergleichbar sind. Solche Verfahren können mittels Brute-Force- oder Wörterbuchangriffen angegriffen werden, selbst dann, wenn zur Ableitung der Schlüssel etablierte und weit verbreitete Ableitungsfunktionen wie PBKDF2 aus dem PKCS#5-Standard [RSA99] verwendet werden. Dies führt dazu, dass ein Angreifer vertrauliche Daten entschlüsseln kann, ohne den zugehörigen Verschlüsselungsalgorithmus (beispielsweise AES) zu brechen. In diesem Zusammenhang wurden in einer aktuellen Studie [BeSk12] 17 Passwortmanager auf mobilen Endgeräten untersucht, die ihre Daten mittels PBE verschlüsseln. Alle 17 Passwortmanager wurden nach spätestens einem Tag geöffnet. Des Weiteren leitet OmniCloud die Verschlüsselungsschlüssel nicht aus dem Dateiinhalt ab. Die Nachteile eines solchen Ansatzes wurden in der Cloud-Studie von Fraunhofer SIT [BHHK$^+$12] beschrieben.

Verschlüsselung. Bei der Verschlüsselung einer Datei werden folgende Schritte ausgeführt: (1) Die Verschlüsselungskomponente erfragt bei der Schlüsselmanagement-Komponente einen neuen Verschlüsselungsschlüssel, (2) die Schlüsselmanagement-Komponente liefert den generierten Schlüssel zusammen mit einer Schlüssel-ID zurück, (3) die Verschlüsselungskomponente verschlüsselt die Datei mit Hilfe des Schlüssels unter Verwendung des konfigurierten Verschlüsselungsverfahrens, (4) die Verschlüsselungskompo-

nente speichert die Schlüssel-ID als interne Meta-Information der Datei für die spätere Entschlüsselung ab.

Entschlüsselung. Die Entschlüsselung einer Datei erfolgt gemäß den folgenden Schritten: (1) Die Entschlüsselungskomponente ermittelt aus den internen Meta-Informationen die Schlüssel-ID der Datei, (2) die Entschlüsselungskomponente erfragt von der Schlüsselmanagement-Komponente den zur Schlüssel-ID gehörigen Schlüssel, (3) die Schlüsselmanagement-Komponente liefert den gewünschten Schlüssel, (4) die Entschlüsselungskomponente entschlüsselt die Datei unter Verwendung des gelieferten Schlüssels.

Die Schlüsselmanagement-Komponente unterstützt die Verwendung von unterschiedlichen Verschlüsselungsverfahren und -modi für verschiedene Dateien. Hierdurch ist es möglich, das in einem OmniCloud-Dienst verwendete Standard-Verschlüsselungsverfahren während des Lebenszyklus eines Dienstes zu wechseln. In einem solchen Fall bleiben die existierenden Dateien weiterhin mit dem alten Verfahren und Schlüssel verschlüsselt, während neue oder veränderte Dateien das neue Verfahren anwenden. Aus Unternehmenssicht ist es somit sehr einfach möglich, ein älteres aber noch sicheres Verschlüsselungsverfahren sukzessive durch ein neues Verfahren abzulösen, ohne dass alle Dateien auf einmal umverschlüsselt werden müssen.

Im Gegensatz zu vielen anderen Verschlüsselungslösungen eignet sich OmniCloud für dynamische Teams und berücksichtigt typische Unternehmenssituationen wie Mitarbeiterausfälle und Änderungen von Zuständigkeiten. Möglich wird dies durch eine Trennung von Identitäts- und Schlüsselmanagement. Hierdurch lassen sich etwa Vertretungsregelungen ganz einfach realisieren – ohne Passwortweitergabe und aufwändige erneute Verschlüsselung der Daten.

4.5. Verschleierung von Datei- und Verzeichnisnamen

Neben dem eigentlichen Inhalt einer Datei können die zugehörigen Meta-Informationen wie der Datei- oder Verzeichnisname ebenfalls vertrauliche Informationen enthalten. Den potentiellen Inhalt einer Datei mit dem Namen *„fristlose-kuendigung-hans-mueller.docx“* kann man auch ohne Blick in die Datei erraten. Auch verrät ein Ordner mit dem Namen *„massnahmen-uebernahme-firma-xyz/“* selbst schon strategische Ziele des Unternehmens. Daher verschlüsselt OmniCloud nicht nur den Inhalt einer Datei, sondern benennt auch alle Dateien um, bevor sie in der Cloud gespeichert werden. Die entsprechenden Dateinamen werden zufällig erzeugt, Dateiendungen wie *„.pdf“* werden entfernt. Des Weiteren wird die komplette Verzeichnisstruktur vor der Speicherung in der Cloud gelöscht und von OmniCloud intern verwaltet. So kann weder ein Angreifer eines Cloud-Speichers noch der Anbieter selbst Rückschlüsse auf die dort gespeicherten Dateien ziehen. Abbildung 5 zeigt beispielhaft den Ordnerinhalt eines von OmniCloud genutzten Cloud-Speichers.

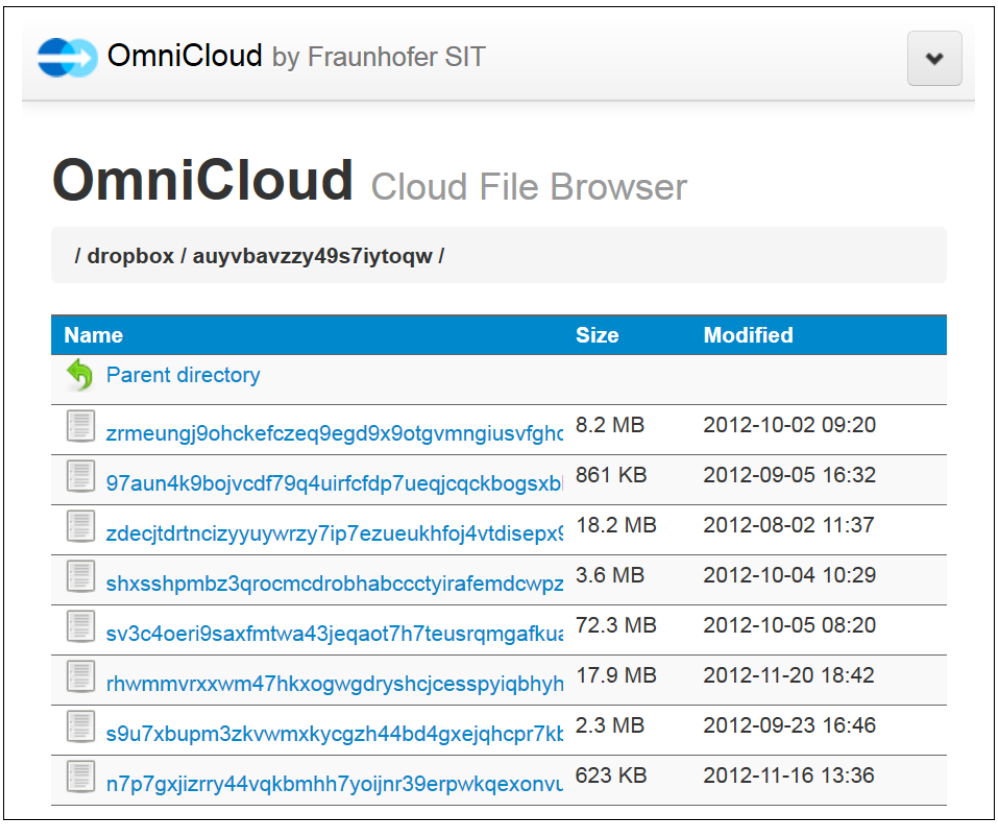

Abbildung 5: Verschleierung von Datei- und Verzeichnisnamen

4.6. Weitere Aspekte von Datensicherheit

Neben den oben beschriebenen Sicherheitsmechanismen sichert OmniCloud alle internen Managementinformationen vor unautorisiertem Zugriff und setzt hierfür geeignete Sicherheitsmechanismen ein (beispielsweise die verschlüsselte Speicherung aller Verschlüsselungsschlüssel). Informationen, die zwischen dem Endgerät des Benutzers und dem OmniCloud-Gateway oder zwischen dem Gateway und dem Cloud-Speicheranbieter ausgetauscht werden, werden durch geeignete Maßnahmen abgesichert (sofern dies durch die eingesetzten Kommunikationsprotokolle oder zusätzliche Maßnahmen möglich ist). Des Weiteren werden alle Datensicherungen von OmniCloud-internen Informationen vor unautorisiertem Zugriff und unbemerkter Veränderung geschützt.

5. Vermeidung von Dopplungen durch Deduplikation

Der Begriff *Deduplikation* beschreibt eine populäre Technik, die es Anbietern von Cloud-Speicherdiensten erlaubt, die Menge an benötigtem Speicherplatz signifikant zu reduzieren. Das Grundprinzip von Deduplikation ist, von jeder Datei nur eine einzige Kopie zu speichern. Wenn ein Nutzer eine Datei speichern möchte, die der Cloud-Speicherdienst

bereits in der Vergangenheit gespeichert hat, wird von dem Dienst lediglich ein Verweis auf die bereits existierende Datei angelegt, anstatt eine weitere Kopie zu speichern. Bei der Realisierung von Deduplikation wird zwischen verschiedenen Varianten unterschieden:

1. **Dateibasierte Deduplikation gegenüber blockbasierter Deduplikation.** Dateibasierte Deduplikation bedeutet, dass nur eine einzige Kopie von jeder Datei gespeichert wird. Bei der blockbasierten Deduplikation dagegen wird jede Datei in Blöcke zerteilt und es wird von jedem dieser Blöcke nur eine einzige Kopie gespeichert. Identische Dateien oder Blöcke werden erkannt, indem deren Hash-Werte mit einer Liste aller bekannten Dateien oder Blöcke verglichen werden.

2. **Server-seitige Deduplikation gegenüber lokaler Deduplikation.** Im Falle server-seitiger Deduplikation wird jede Datei, die ein Nutzer speichern möchte, zunächst an den Cloud-Speicherdienst gesendet. Der Dienst prüft für jede Datei, ob sie gespeichert werden muss oder lediglich ein Verweis auf eine bereits existierende Datei angelegt werden braucht. Der Nutzer kann in diesem Fall nicht erkennen, ob der Cloud-Speicherdienst Deduplikation unterstützt. Im Falle lokaler Deduplikation sendet die Client-Anwendung zunächst nur den Hash-Wert der Datei an den Dienst. Nur wenn der Dienst die Datei noch nicht besitzt, wird die Client-Anwendung anschließend aufgefordert, die komplette Datei zu senden. Diese Art der Deduplikation hat den Effekt, dass nicht nur Speicherplatz eingespart wird, sondern auch Bandbreite. Durch eine Analyse der Log-Dateien oder durch Beobachtung der übertragenen Daten ist einfach zu erkennen, ob ein Dienst diese Art der Deduplikation verwendet.

3. **Deduplikation pro Nutzer gegenüber nutzerübergreifender Deduplikation.** Deduplikation pro Nutzer bedeutet, dass Deduplikation separat für jeden einzelnen Nutzer durchgeführt wird: Wenn Nutzer A eine Datei speichern möchte, die er selbst bereits in der Vergangenheit gespeichert hat (möglicherweise in einem anderen Verzeichnis), erzeugt der Cloud-Speicherdienst lediglich einen Verweis auf die Datei. Wurde die Datei jedoch nur von einem anderen Nutzer bereits gespeichert, wird eine weitere Kopie der Datei angelegt. Bei der nutzerübergreifenden Deduplikation ist dies nicht so. Hier wird Deduplikation über alle Nutzer hinweg durchgeführt: Der Cloud-Speicherdienst legt auch dann einen Verweis auf eine bereits existierende Datei an, wenn Nutzer A eine Datei speichern möchte, die ein anderer Nutzer B bereits gespeichert hat.

Durch die Verwendung von OmniCloud können Nutzer von den Vorteilen der Deduplikation profitieren, selbst wenn der Cloud-Speicherdienst keine Deduplikation unterstützt. Da OmniCloud die Hash-Werte aller Dateien speichert, ist OmniCloud in der Lage zu entscheiden, ob eine Datei bereits an einen Cloud-Speicherdienst übertragen wurde oder nicht. Wenn eine Datei bereits an einen Cloud-Speicherdienst gesendet wurde, legt OmniCloud einen Verweis in der eigenen Datenbank an und markiert die Datei

damit als dedupliziert. OmniCloud führt Deduplikation für jeden OmniCloud-Dienst separat durch. Das bedeutet, dass, in Abhängigkeit von der Gruppe der autorisierten Nutzer eines Dienstes, sowohl Deduplikation pro Nutzer als auch nutzerübergreifende Deduplikation möglich sind.

Es existieren jedoch auch einige Datenschutzprobleme, die bei der Verwendung von Deduplikation beachtet werden sollten [HaPSP10]. Diese Datenschutzprobleme können allerdings nur auftreten, wenn der Cloud-Speicherdienst sowohl lokale als auch nutzerübergreifende Deduplikation verwendet. Ist dies der Fall, sind einige Seitenkanalangriffe möglich. Diese Angriffe funktionieren nach dem folgenden Prinzip: Ein Angreifer, der einen Zugang zu einem Cloud-Speicherdienst besitzt, kann Deduplikation nutzen, um zu lernen, welche Dateien bereits bei diesem Dienst gespeichert wurden: Er sendet eine Datei an den Dienst und beobachtet, was passiert. Wenn seine Client-Anwendung die Datei nicht überträgt, weiß der Angreifer, dass diese Datei bereits bei dem Cloud-Speicherdienst vorhanden ist. Genauer gesagt weiß er, dass zumindest ein anderer Nutzer die gleiche Datei besitzt, er weiß jedoch nicht welcher. Ausgefeiltere Varianten dieses Angriffs nutzen dieses Prinzip, um Informationen über einen bestimmten Nutzer zu erlangen.

OmniCloud verhindert jedoch diese Angriffsarten. Zunächst einmal führt OmniCloud aus Sicht der Client-Anwendung eine server-seitige Deduplikation aus, da der Client jede Datei an OmniCloud übertragen muss, gleichgültig, ob diese Datei bereits in der Vergangenheit übertragen wurde oder nicht. Außerdem wird Deduplikation nur innerhalb eines OmniCloud-Dienstes durchgeführt. Auf einen OmniCloud-Dienst haben jedoch nur Nutzer Zugriff, die sich untereinander ein hohes Maß an Vertrauen entgegenbringen, weshalb Seitenkanalinformationen als nicht besonders kritisch anzusehen sind. Um diese Informationsflüsse trotz allem zu unterbinden, kann entweder für jeden Nutzer ein eigener OmniCloud-Dienst eingerichtet werden oder Deduplikation wird für einzelne OmniCloud-Dienste deaktiviert.

6. Leichter Anbieterwechsel durch Umzugsdienst

Ein wesentlicher Grund, weshalb viele Unternehmen zögern, Cloud-Speicherdienste einzusetzen, ist die Furcht, sich an einen Cloud-Anbieter zu binden („Provider Lock-in“). Da es im Allgemeinen kein effizientes Verfahren für eine Migration der Daten zwischen verschiedenen Cloud-Anbietern gibt, sind Benutzer in der Regel an den Cloud-Anbieter gebunden, den sie anfangs ausgewählt haben. Um dem entgegenzuwirken, bietet OmniCloud einen sogenannten Umzugsdienst an, der den Nutzern hilft, einfach zu einem anderen Cloud-Speicherdienst zu wechseln.

Ein besonderes Merkmal des Umzugsdienstes ist, dass er nicht Bestandteil des lokalen OmniCloud-Gateway ist. Stattdessen läuft er als virtuelle Maschine bei einem Cloud-Anbieter außerhalb des Unternehmens-Intranets. Das lokale OmniCloud-Gateway steuert lediglich den Umzugsdienst. Wenn eine Datenmigration ausgeführt wird, nimmt

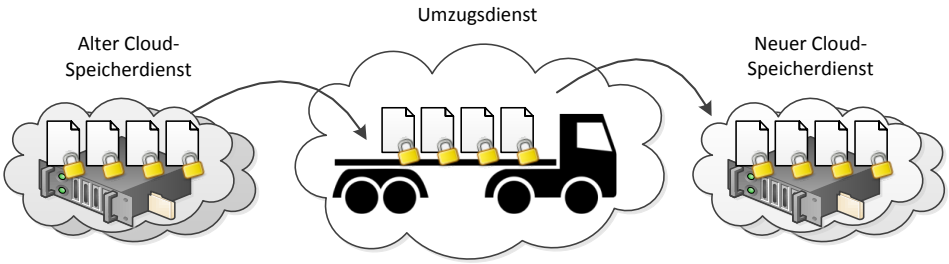

Abbildung 6: Umzugsdienst von OmniCloud

der Umzugsdienst alle verschlüsselten Dateien von dem alten Cloud-Speicherdienst und überträgt sie zu dem neuen Dienst (vgl. Abbildung 6). Es ist nicht notwendig, die Dateien zu entschlüsseln und anschließend wieder neu zu verschlüsseln.

Der Vorteil gegenüber einem Umzugsdienst, der innerhalb des Unternehmens-Intranets läuft, ist, dass diese Lösung sehr stark von den High-Speed-Internet-Verbindungen zwischen Cloud-Diensten profitiert. Wenn beispielsweise ein lokaler Umzugsdienst über eine eher langsame DSL-Verbindung alle Dateien mit einer Gesamtgröße von 500 GB vom Cloud-Speicherdienst A herunterladen und anschließend zu Dienst B hochladen würde, dann würde die Zeit für den Datentransfer mehr als sieben Wochen in Anspruch nehmen [3]. Zudem wäre während des Datentransfers das lokale Intranet sehr stark belastet, wodurch die Verwendung des lokalen OmniCloud-Gateway, das im selben Intranet läuft, eingeschränkt werden könnte. Dagegen steigt die Übertragungsgeschwindigkeit dramatisch an, wenn Daten direkt von Cloud zu Cloud kopiert werden. Eine Analyse von Nasuni kam zu dem Ergebnis, dass das Kopieren von 12 TB Daten von einer Cloud zu einer anderen nur zwischen vier Stunden und einer Woche dauert [Nasu12].

[3] Basis für die Berechnung: DSL 16.000 mit einer Netto Download-Rate von 1 MB/sek. und einer Netto Upload-Rate von 128 KB/sek.

Literatur

[AbPW10] H. Abu-Libdeh, L. Princehouse und H. Weatherspoon. RACS: A Case for Cloud Storage Diversity. In *Proc. of the 1st ACM Symp. on Cloud Comp.* ACM, 2010, S. 229–240.

[AlWo09] C. Alm und R. Wolf. The Definition of the OPL Access Control Policy Language. Technical Report MIP-0902, University of Passau, Germany, 2009.

[AlWP09] C. Alm, R. Wolf und J. Posegga. The OPL Access Control Policy Language. In *TRUSTBUS*, Band 5695 der *LNCS*. Springer, 2009, S. 138–148.

[Amaz] Amazon Web Services. Amazon Simple Storage Service (Amazon S3). http://aws.amazon.com/de/s3/ (Abruf 1.11.2012).

[BeSk12] A. Belenko und D. Sklyarov. "Secure Password Managers" and "Military-Grade Encryption" on Smartphones: Oh, Really? http://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf (Abruf: 1.11.2012), März 2012.

[BHHK+12] M. Borgmann, T. Hahn, M. Herfert, T. Kunz, M. Richter, U. Viebeg und S. Vowé. On the Security of Cloud Storage Services. SIT Technical Reports SIT-TR-2012-001, http://www.sit.fraunhofer.de/de/cloudstudy.html (Abruf: 1.11.2012), März 2012.

[BSI12] BSI. Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile (Abruf: 1.11.2012), Januar 2012.

[Capg12] Capgemini. Studie IT-Trends 2012. Business-IT-Alignment sichert die Zukunft. http://www.de.capgemini.com/insights/publikationen/it-trends-2012/ (Abruf: 1.11.2012), Januar 2012.

[Cons12] J. Constine. Dropbox Is Now The Data Fabric Tying Together Devices For 100M Registered Users Who Save 1B Files A Day. TechCrunch, Available from http://techcrunch.com/2012/11/13/dropbox-100-million/ (Abruf 19.11.2012), November 2012.

[Deut11] Deutsche Telekom / T-Systems. Sicherheitsreport 2011. http://www.telekom.com/static/-/22846/1/110916-sicherheitsreport-si (Abruf: 1.11.2012), September 2011.

[Duss07] L. Dusseault. RFC 4918: HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV), Juni 2007.

[Fiel00] R. Fielding. *Architectural Styles and the Design of Network-based Software Architectures.* Dissertation, University of California, Irvine, 2000.

[File] FileZilla Wiki. SFTP specifications. Available from http://wiki.filezilla-project.org/SFTP_specifications (Abruf 1.11.2012).

[HaPSP10] D. Harnik, B. Pinkas und A. Shulman-Peleg. Side Channels in Cloud Services: Deduplication in Cloud Storage. *IEEE Sec. & Priv.* 8(6), November 2010, S. 40–47.

[HeLP96] I. Heizer, P. Leach und D. Perry. Common Internet File System Protocol (CIFS/1.0). Internet Draft. Available from http://tools.ietf.org/html/draft-heizer-cifs-v1-spec-00 (Abruf 1.11.2012), Juni 1996.

[Nasu12] Nasuni. Bulk Data Migration in the Cloud. Whitepaper, http://www.nasuni.com/cloud-migration (Abruf: 1.11.2012), März 2012.

[NeSt04] G. Neumann und M. Strembeck. An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments. *ACM TISSEC* 7(3), 2004, S. 392–427.

[Orac] Oracle. Jan Pechanec's weblog: How the SCP protocol works. https://blogs.oracle.com/janp/entry/how_the_scp_protocol_works (Abruf 1.11.2012).

[PoRe85] J. Postel und J. K. Reynolds. RFC 959: File Transfer Protocol, Oktober 1985.

[RSA99] RSA. PKCS #5 v2.0: Password-Based Cryptography Standard, März 1999.

[SeGS11] R. Seiger, S. Groß und A. Schill. SecCSIE: A Secure Cloud Storage Integrator for Enterprises. In *Commerce and Enterprise Computing (CEC), 2011 IEEE 13th Conference on.* IEEE, 2011, S. 252–255.

[Sp+ot11] J. Spillner und andere. Information Dispersion over Redundant Arrays of Optimal Cloud Storage for Desktop Users. In *Proc. of Utility and Cloud Computing (UCC) 2011.* IEEE, 2011, S. 1–8.

[WoKS03] R. Wolf, T. Keinz und M. Schneider. A Model for Context-dependent Access Control for Web-based Services with Role-based Approach. In *DEXA Intern. Workshop on Network-Based Information Systems.* IEEE Computer Society Press, 9 2003, S. 209–214.

A. Häufig gestellte Fragen (FAQ)

Allgemeine Fragen

1. **Was ist OmniCloud?**

   OmniCloud ist eine Lösung, welche die sichere und flexible Nutzung beliebiger Cloud-Speicherdienste für Unternehmen ermöglicht.

2. **Von wem wird OmniCloud entwickelt?**

   OmniCloud wird vom Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt entwickelt.

3. **Ist OmniCloud ein Cloud-Speicherdienst?**

   Nein, OmniCloud ist keine Konkurrenz für Cloud-Speicherdienste. OmniCloud speichert selbst keine Dateien, sondern verschlüsselt sie und leitet sie an existierende Cloud-Speicherdienste weiter.

4. **Mit welchen Cloud-Speicheranbietern arbeitet OmniCloud zusammen?**

   Derzeit unterstützt OmniCloud Amazon S3, Dropbox, Box und beliebige FTP-Server. Weitere Anbieter folgen in Kürze.

5. **Kann ich OmniCloud auch mit lokalem Speicherplatz verwenden?**

   OmniCloud unterstützt sowohl lokalen als auch Cloud-Speicher. Lokaler Speicher kann beispielsweise mittels FTP oder direkt über Dateisystem-Schnittstelle angebunden werden.

Lizensierung, Kauf und Vertrieb

6. **Wie ist der aktuelle Status von OmniCloud?**

   OmniCloud befindet sich noch in der Entwicklung. Das Konzept und der OmniCloud-Prototyp wurden von Fraunhofer SIT entwickelt und bei zahlreichen Veranstaltungen vorgestellt. Fraunhofer SIT plant, OmniCloud zu einem real verwert- und vermarktbaren Produkt weiter zu entwickeln.

7. **Wie kann ich OmniCloud kaufen oder lizensieren?**

   Die Software-Entwicklung und Produktisierung von OmniCloud dauert an. Derzeit finden Gespräche mit potenziellen Vertriebspartnern statt. Das Lizenzierungsmodell ist derzeit noch nicht fertiggestellt.

8. **Wie kann ich als Systemhaus oder Systemintegrator selbst ein Vertriebspartner für OmniCloud werden?**

   Bitte bewerben Sie sich hierfür bei uns. Unsere Kontaktdaten finden Sie am Ende dieses Dokuments.

9. **Ich interessiere mich für den Einsatz von OmniCloud in unserem Unternehmen. Wie erhalte ich Informationen, sobald OmniCloud fertig ist?**

   Gerne informieren wir Sie über Neuigkeiten zu OmniCloud. Bitte schicken Sie uns hierfür eine kurze Nachricht. Unsere Kontaktdaten finden Sie am Ende dieses Dokuments.

10. **Ich möchte gerne einen Artikel über OmniCloud in einer Zeitschrift oder einem Blog verfassen, woher bekomme ich weitere Informationen zu OmniCloud?**

    Viele Details zu OmniCloud sind bereits in diesem Whitepaper und auf unserer OmniCloud-Webseite unter http://www.sit.fraunhofer.de/omnicloud dargestellt. Sollten Sie weitere Informationen benötigen, dann nehmen Sie bitte Kontakt mit uns auf. Unsere Kontaktdaten finden Sie am Ende dieses Dokuments.

Installation und Benutzung

11. **Wo wird OmniCloud installiert?**

    OmniCloud wurde für die Nutzung in Unternehmen entworfen. Hierfür muss die OmniCloud-Software im Unternehmensnetzwerk auf einem Server, dem sogenannten OmniCloud-Gateway, installiert werden. Alle OmniCloud-Benutzer können dann über dieses Gateway auf den sicheren Cloud-Speicher zugreifen.

12. **Welches Betriebssystem benötige ich auf meinem Endgerät, um mit OmniCloud arbeiten zu können?**

    OmniCloud kann unabhängig von einem bestimmten Betriebssystem genutzt werden. Für alle gängigen Betriebssysteme gibt es Applikationen, die Standard-Protokolle (wie CIFS, FTP, SFTP, SCP, Amazon S3, u. a.) unterstützen und für die Kommunikation mit OmniCloud verwendet werden können.

13. **Ist die Installation einer OmniCloud-Applikation auf dem Endgerät jedes Benutzers notwendig? Wie greifen Benutzer auf OmniCloud zu?**

    Um OmniCloud nutzen zu können, brauchen Sie keine OmniCloud-Applikation zu installieren. Nutzen Sie stattdessen Standard-Software wie einen Dateimanager oder eine Backup-Software, um mit OmniCloud über Standard-Protokolle (wie

CIFS, FTP, SFTP, SCP, Amazon S3, u. a.) zu kommunizieren. Viele Betriebssysteme erlauben es, Netzwerkressourcen für alle lokalen Anwendungen verfügbar zu machen.

14. Können die mit OmniCloud gespeicherten Daten gemeinsam benutzt werden?

Ja. OmniCloud stellt sich dem Benutzer ähnlich wie ein Netzlaufwerk dar, auf das verschiedene Benutzer zugreifen können.

15. Können beispielsweise auch Mitarbeiter, die im Außendienst tätig sind, auf die mit OmniCloud in der Cloud gespeicherten Daten zugreifen?

Ja. Hierfür muss sich der Mitarbeiter zunächst, wie bei der Nutzung anderer Intranetdienste auch, mittels eines VPN-Tunnels mit dem Unternehmensnetzwerk verbinden. Alternativ können einzelne OmniCloud-Dienste auch durch eine Portfreischaltung der Firewall nach außen verfügbar gemacht werden. In jedem Fall ist aber eine Authentifizierung des Benutzers notwendig.

16. Kann OmniCloud genutzt werden, um Dateien für externe Geschäftspartner freizugeben?

Ja. Sofern für die Geschäftspartner ein Zugang zu OmniCloud eingerichtet wurde, können diese auf einzelne OmniCloud-Dienste zugreifen. Hierfür ist eine Authentifizierung der Geschäftspartner gegenüber OmniCloud notwendig. Mit Hilfe von Zugriffsregeln kann feingranular festgelegt werden, welche Geschäftspartner Zugriff auf welche Dateien haben.

17. Wie komme ich an meine Dateien, wenn mein Endgerät defekt ist?

Kein Problem. Melden Sie sich hierfür mit einem anderen Endgerät und Ihren Zugangsdaten beim OmniCloud-Gateway an. Sie erhalten dann sofort wieder Zugang zu ihren Dateien.

18. Kann OmniCloud mehrere Versionen einer Datei verwalten?

Nein, derzeit leider nicht.

19. Entstehen während des Betriebs von OmniCloud laufende Kosten für das Unternehmen?

Zusätzlich zu den OmniCloud-Lizenzkosten fallen ggf. Kosten für die Speicherung, den Abruf und die Übertragung der Dateien bei den genutzten Cloud-Speicheranbietern an. Bei der Nutzung des OmniCloud-Umzugsdienstes fallen ggf. weitere Kosten für den Transfer der Dateien vom alten zum neuen Cloud-Speicheranbieter an.

Sicherheit

20. Kann ein Cloud-Anbieter herausfinden, um welche Daten es sich handelt?

Nein. OmniCloud verschlüsselt den Inhalt der Datei. Zudem werden Dateinamen und die Dateiendungen durch zufällige Bezeichner ersetzt und Verzeichnisstrukturen entfernt.

21. Welches Verschlüsselungsverfahren wird von OmniCloud eingesetzt?

OmniCloud unterstützt verschiedene symmetrische Verschlüsselungsverfahren. Standardmäßig wird AES-256 eingesetzt.

22. Wo werden die Daten verschlüsselt?

Die Daten werden innerhalb des Unternehmensnetzwerks auf dem OmniCloud-Gateway verschlüsselt, bevor sie an den Cloud-Speicheranbieter übermittelt werden.

23. Werden alle Dateien mit dem gleichen Schlüssel verschlüsselt?

Nein. OmniCloud generiert für jede Datei einen eigenen Schlüssel. Sogar beim Aktualisieren einer Datei wird ein neuer Schlüssel generiert.

24. Werden die Verschlüsselungsschlüssel aus dem Namen oder dem Inhalt der zu verschlüsselnden Datei abgeleitet?

Nein. OmniCloud generiert alle Schlüssel (pseudo-)zufällig. Die erzeugten Schlüssel haben keinen Bezug zum Namen oder Inhalt der Datei. Gäbe es einen solchen Bezug, dann könnte sich das negativ auf die Sicherheit und den Datenschutz auswirken.

25. Muss ich als OmniCloud-Nutzer alle Schlüssel selbst verwalten?

Nein, OmniCloud kümmert sich um das gesamte Schlüsselmanagement.

26. Sind alle Schlüssel verloren, wenn mein Endgerät kaputt geht?

Nein, die Schlüssel sind nicht auf dem Endgerät des Benutzers gespeichert sondern auf dem OmniCloud-Gateway.

27. Haben alle OmniCloud-Benutzer Zugriff auf meine gespeicherten Daten?

Nein. Mit Hilfe von Zugriffsregeln kann genau festgelegt werden, welcher Benutzer auf welche Daten zugreifen darf.

28. Wie melde ich mich bei OmniCloud an?

Das konkrete Anmeldeverfahren hängt von den konfigurierten Input-Modulen ab (bei dem FTP-Input-Modul beispielsweise mittels Benutzername und Passwort). Benutzer erhalten hierfür eigene Zugangsberechtigungen für die Nutzung einzelner OmniCloud-Dienste.

Über Fraunhofer SIT

Das Fraunhofer-Institut für Sichere Informationstechnologie SIT gehört zu den ältesten und angesehensten Forschungseinrichtungen zu IT-Sicherheit in der Welt. Über 165 Mitarbeiter unterstützen Unternehmen und Behörden bei der Absicherung von Daten, Diensten, Infrastrukturen und Endgeräten.

Fraunhofer SIT betreibt Anwendungsforschung mit dem Ziel, neue Technik so zur Marktreife zu bringen, dass sich deren Potenziale sicher und vollständig nutzen lassen. Zusammen mit seinen Partnern arbeitet das Institut an neuen Methoden und Verfahren, erstellt Prototypen, entwickelt individuelle IT-Lösungen und testet bestehende Produkte und Systeme.

Kontakt

Fraunhofer-Institut für Sichere
Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Tel.: 06151 869-213
Fax: 06151 869-224
info@sit.fraunhofer.de
www.sit.fraunhofer.de

Ansprechpartner für OmniCloud

Thomas Kunz
Tel.: 06151 869-164
Fax: 06151 869-224
omnicloud-info@sit.fraunhofer.de

Ruben Wolf
Tel.: 06151 869-178
Fax: 06151 869-224
omnicloud-info@sit.fraunhofer.de

OmniCloud-Webseite

www.sit.fraunhofer.de/omnicloud