



Warum Sie ownCloud brauchen

Stand-alone oder als zusätzliche strategische Filesharing-Plattform
neben MS OneDrive

Ziel

Unternehmen wollen Ihren Mitarbeitern eine reibungslose Zusammenarbeit ermöglichen und die Produktivität steigern – bei gleichzeitiger Kosteneinsparung (Reduzierung der Storage-Kosten, Senkung der Betriebs- und Personalkosten).

Teillösung

Überführen von Desktop-Anwendungen in die Cloud. Das beliebteste Angebot ist Microsoft Office 365, das zusammen mit OneDrive zum Speichern und Teilen von Dateien angeboten wird.

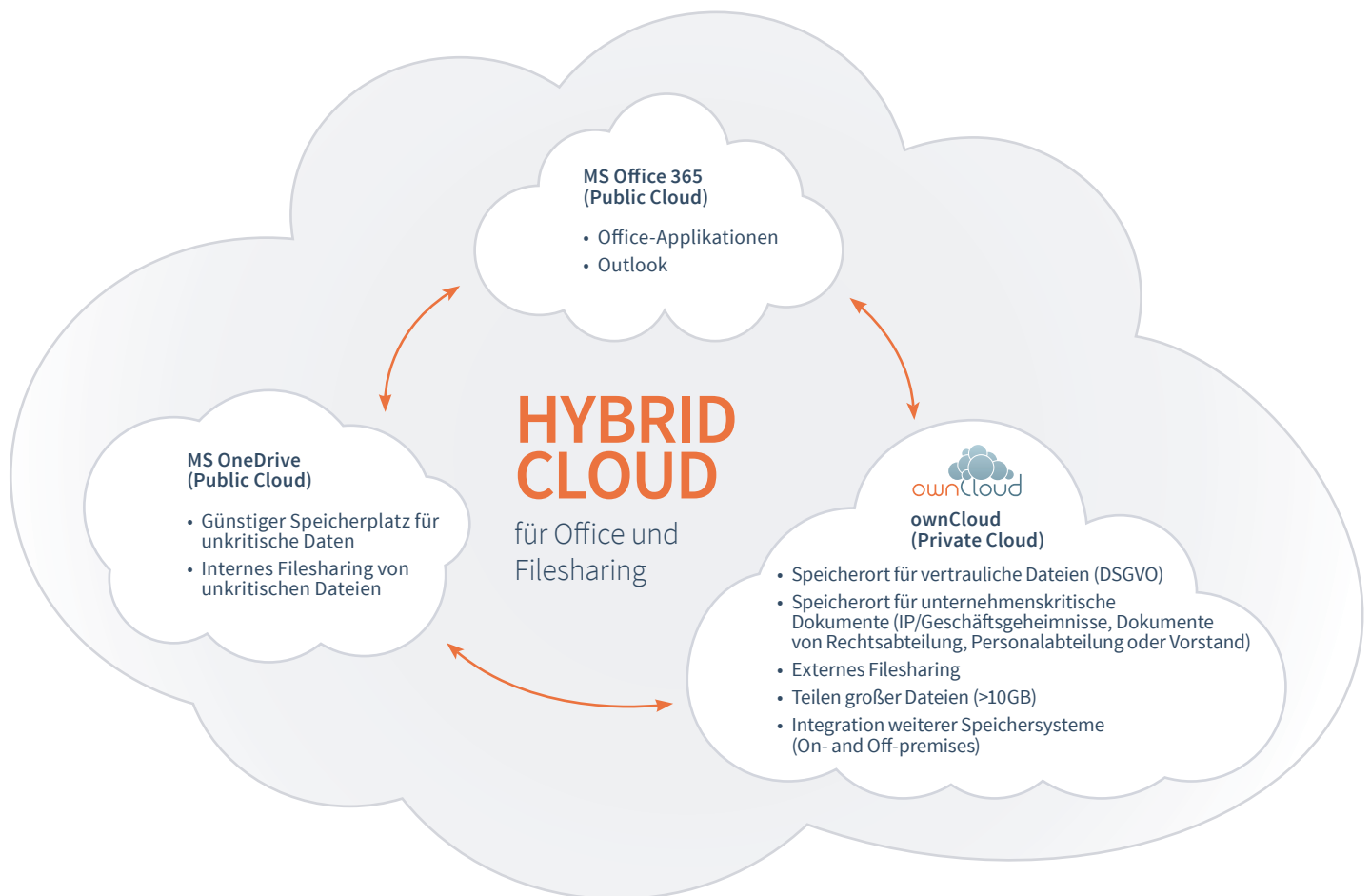
Fakten

Basierend auf dem „Cloud Act“ kann die US-Regierung auf alle Daten zugreifen, die in Clouds von US-Anbietern wie Microsoft, Amazon, Google, Dropbox etc. gespeichert sind – unabhängig vom Standort des

Rechenzentrums (innerhalb oder außerhalb der USA). Die Trump-Administration untersagte kürzlich Google die Zusammenarbeit mit Huawei. Im Zusammenhang mit dem schwelenden Handelsstreit zwischen den USA und Europa oder mit Strafverfolgungsmaßnahmen könnte sie somit auch für europäische Unternehmen den Zugriff auf Daten einschränken, die in Clouds von US-Anbietern gespeichert sind.

„Können wir ausschließen, dass eines Tages gedroht wird, die Cloud-Dienste quasi zu kappen, wenn Deutschland nicht die Nord-Stream-2-Leitung ebenfalls kapt?“

*Karl-Heinz Streibich,
Präsident der Deutschen Akademie der Technikwissenschaften*



State-of-the-art Hybrid-Cloud für Office und Filesharing: Sensible Dateien bleiben in der Private Cloud.

Herausforderung

- 1 Microsoft hat seit 2018 Schwierigkeiten mit der EU-DSGVO. Nach Einschätzung des niederländischen Justizministeriums ist MS Office 365/OneDrive nicht DSGVO-konform! <https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office>

Hauptgrund: MS Office 365/OneDrive erweist sich als intransparent in Bezug auf die Art der an Microsoft gesendeten (Telemetrie-)Daten, so dass der Administrator/Benutzer nicht feststellen kann, wo und wie lange sensible Daten gespeichert sind.

Wichtig: Das kürzlich eingeführte Privacy Dashboard (nur für Windows 10) schließt das Risiko eines Verstoßes gegen die DSGVO nicht aus. Denn Microsoft veröffentlicht regelmäßig und ohne vorherige Ankündigung neue Funktionen in Office 365/OneDrive, und es gibt keine Möglichkeit, durch diese neuen Funktionen verursachte DSGVO-Verstöße zu verhindern. So kann ein System zu einem bestimmten Zeitpunkt DSGVO-konform sein und schon am nächsten Tag gegen die DSGVO verstoßen. Darüber hinaus enthält die DSGVO als einen ihrer Kernpunkte die Verpflichtung, eine Datenschutz-Folgenabschätzung (DSFA) für solche Verarbeitungstätigkeiten durchzuführen, die ein „hohes Risiko“ für die Privatsphäre von Personen darstellen (Artikel 35). Datenschutz-Folgenabschätzung stellen einen wichtigen Aspekt der DSGVO-Konformität dar und sind für alle Daten verpflichtend, die in Blacklists (siehe Anhang) der Europäischen Datenschutzbehörden (DSB) enthalten sind. Aufgrund des „Cloud Acts“ (<https://owncloud.com/cloud-act-passed-by-us-congress/>), der es der US-Regierung ermöglicht, unabhängig von ihrem Speicherort auf alle Daten zuzugreifen, die in Clouds von US-Anbietern wie Microsoft gespeichert sind, muss das Ergebnis aller DSFA negativ sein. Das bedeutet, dass alle Daten, die in den Blacklists der Datenschutzbehörden enthalten sind, nicht in MS OneDrive gespeichert werden dürfen. Prominente Beispiele sind Personaldaten, Patientenakten und Überwachungsvideos.

- 2 Aufgrund des „Cloud Acts“ sollten sensible Informationen wie geistiges Eigentum, Geschäftsgeheimnisse, rechtliche Dokumente und sämtliche Arten von Vorstandsdokumenten nicht in einer US-Cloud wie MS OneDrive gespeichert werden. Die US-Regierung kann alle Datenzugriffe allein mit Hilfe der nationalen Sicherheit rechtfertigen! Es gibt kein Kontrollorgan, und es muss beim Datenzugriff weder eine Beratung noch eine Offenlegung stattfinden. Seit Snowden ist bekannt, dass die US-Regierung den Zugriff auf solche Daten nicht scheut. Durch den „Cloud Act“ ist es unerheblich, in welchem Land die Daten gespeichert sind.
- 3 Public Cloud-Plattformen wie Microsoft Office 365/ OneDrive bieten eine gute Integration zwischen den eigenen Anwendungen, haben aber naturgemäß enge Grenzen bei der Integration von kundenspezifischen IT-Infrastrukturen. Dies führt zur Einschränkung der Anwendungsfälle, die mit Microsoft Office 365/OneDrive abgedeckt werden können. Jede größere Organisation oder Firma hat Filesharing-Anwendungsfälle, die mit MS OneDrive nicht umsetzbar sind.
- 4 Wenn Sie im Bereich Filesharing und Storage nur auf einen einzigen Anbieter setzen, resultiert das in einem Vendor-Lock-in. Diese Art der Bindung an einen Lieferanten stellt ein Risiko für Ihr Unternehmen dar.

Komplettlösung

Einsatz von ownCloud entweder als

- (a)** sicherer On-Premises-Speicherort und Filesharing-Ersatz für OneDrive oder
- (b)** zweite strategische Filesharing-Plattform neben OneDrive – um alle sensiblen Daten zu speichern und alle Anwendungsfälle bedienen zu können, die von einer Public Cloud-Plattform wie OneDrive nicht abgedeckt werden können, sowie außerdem um ein Vendor-Lock-in zu vermeiden.

ownCloud ist Ihre einzige oder zusätzliche strategische Filesharing-Plattform, wenn Sie

- 1 Daten speichern und teilen, die auf den Blacklists der Datenschutzbehörden stehen
- 2 vertrauliche Daten speichern und mit anderen teilen, die für die US-Regierung nicht zugänglich sein sollen oder dürfen
- 3 besondere Datenschutzbestimmungen einhalten müssen
- 4 Lösungen für spezielle Anwendungsfälle bereitstellen müssen, die mit OneDrive nicht umsetzbar sind, oder wenn andere Applikationen um File-sharing-Funktionalitäten erweitert werden sollen (z. B. Filesharing innerhalb eines Lieferantenportals)
- 5 Dateien sicher mit externen Partnern teilen müssen (das bedeutet: nicht über öffentliche Links), diese externen Nutzer jedoch nicht in Ihrem Active Directory oder Ihrer Domain angelegt werden sollen
- 6 große Dateien (> 10 GB) oder große Mengen an Dateien teilen müssen
- 7 Infrastrukturkomponenten (z. B. spezifische Authentifizierungssysteme, Windows Netzwerklaufwerk, FTP-Server usw.) integrieren müssen
- 8 eine leicht bedienbare Ende-zu-Ende-Verschlüsselung bereitstellen wollen
- 9 die Plattform auch autonom (also unabhängig von einer Internetverbindung) betreiben müssen
- 10 zu 100% sicher sein müssen, dass die Software keine „Hintertüren“ enthält und dies auch nachweisen müssen
- 11 eine Filesharing-Plattform (inkl. Clients/Apps) im Design Ihres Unternehmens bereitstellen wollen
- 12 Ihr „Dropbox-Problem“ lösen müssen (Mitarbeiter verwenden private Dropbox-Accounts, um Firmendokumente bequem zu speichern und mit externen Personen zu teilen)
- 13 regelmäßig Dateien mit Gast-Nutzern teilen müssen (solche Gast-Accounts haben volle Funktionalität und Auditierbarkeit aber kein eigenes Speicherkontingent) und Sie für diese Gast-Accounts nicht voll bezahlen möchten
- 14 Daten von mehreren externen Parteien komfortabel sammeln müssen (File Drop)
- 15 Daten aus Cloud-Speicherdiensten, wie z. B. Dropbox, Box oder Google Drive, migrieren müssen
- 16 eine Hybrid-Cloud-Strategie umsetzen müssen, bei der sensible (vertrauliche) Daten ausschließlich in On-Premises-Speicherorten verbleiben
- 17 eine kosteneffiziente Filesharing-Lösung für viele interne und externe Endanwender bereitstellen müssen
- 18 Dokumente ohne Downloadmöglichkeit teilen müssen (sicheres Anzeigen am Bildschirm mit einem integrierten Wasserzeichen, das eine eindeutige Nutzerkennung beinhaltet)
- 19 in der Lage sein müssen, auf Administrator-Ebene die Lebensdauer von Dateien festzulegen (z. B. für die DSGVO-Konformität)

Was weder Microsoft noch Google bieten können:

- 1 Unbegrenzte Dateigröße
- 2 Branding
- 3 Flexibilität/Integration
- 4 Dateizugriffskontrolle
- 5 Open Source Software (auditierbar)
- 6 Secure View (Nur-Lese-Zugriff in Form einer per Wasserzeichen geschützten Darstellung am Bildschirm)

WARUM SIE OWNCLLOUD BRAUCHEN

Integration in MS Office/OneDrive:

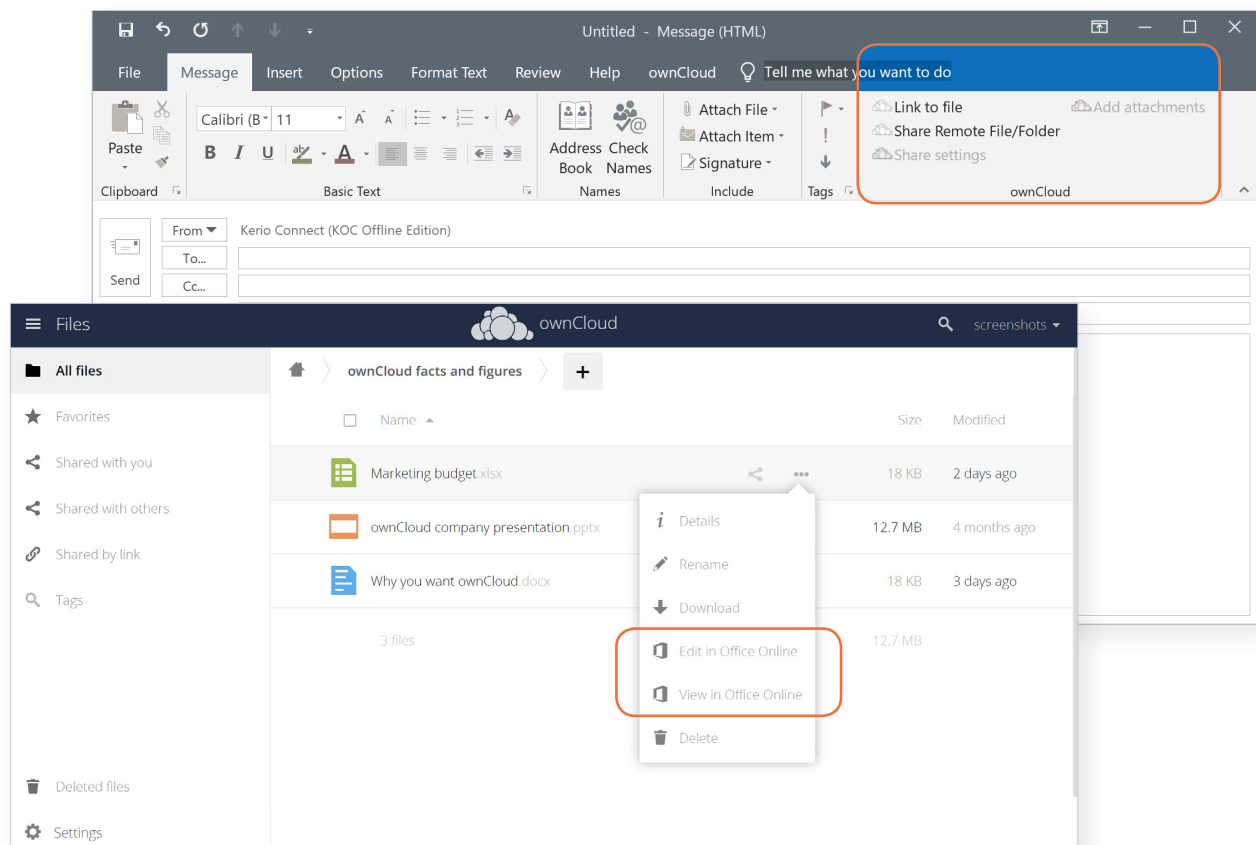
ownCloud lässt sich nahtlos in MS Office 365 und OneDrive integrieren, um die bestmögliche Benutzerfreundlichkeit zu gewährleisten. Zum Beispiel können Nutzer:

- Via ownCloud auf Dateien zugreifen, die in OneDrive gespeichert sind
- MS Office-Dokumente in ownCloud bearbeiten (auch gemeinsam mit anderen Kollegen, dank des MS Office Online Servers)
- Ordner und Dateien direkt aus MS Outlook heraus teilen (über das Outlook-Plugin)

Wahlmöglichkeiten / Zukunftssicherheit:

ownCloud ist der einzige Anbieter, der Kunden völlige Freiheit lässt, wo und wie die Implementierung erfolgen soll:

- 100% On-Premises
- 100% bei einem Hosting-Partner Ihres Vertrauens
- 100% in der Public Cloud (Amazon, Azure, ...)
- Hybrid: ownCloud Management in Ihrer geschützten IT-Umgebung und verschlüsselte Daten in der Public Cloud: Behalten Sie die Kontrolle über Ihre Metadaten, Schlüssel, Verschlüsselungsalgorithmen usw. und profitieren Sie gleichzeitig von der kostengünstigen Speicherung in der Public Cloud.



Fazit

- Mit ownCloud können Sie aktuelle und zukünftige Anforderungen erfüllen, die mit MS OneDrive nicht abgedeckt werden können.
- ownCloud ist perfekt in MS Office / OneDrive integriert und daher die erste Wahl als zweite strategische Filesharing-Plattform.
- Mit ownCloud vermeiden Sie ein riskantes und teures Vendor-Lock-in.
- ownCloud ist so offen und flexibel, dass teure Individuallösungen für spezielle Anwendungsfälle überflüssig sind.
- ownCloud ist mit über 50 Millionen Nutzern die größte Open Source Filesharing-Lösung der Welt. Unterstützt wird sie von der ownCloud Foundation, die die Nachhaltigkeit der Lösung garantiert.

Anhang

Daten, die aufgrund des Cloud Act nicht in MS OneDrive gespeichert werden können:

Alle Daten, die lt. DSGVO (Artikel 35) der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) unterliegen, können nicht in MS OneDrive gespeichert werden, da die US-Regierung aufgrund des Cloud Acts Zugriff darauf haben könnte.

Die nationalen Datenschutzbehörden (DSB) definieren, welche Arten von Daten unter Artikel 35 fallen.

Die DSGVO gewährt Datenschutzbehörden eine gewisse Flexibilität bei der Bestimmung, wann Unternehmen in ihrem Zuständigkeitsbereich eine DSFA durchführen müssen und wann nicht. Artikel 35 Absatz 4 erlaubt es den Datenschutzbehörden, „Blacklists“ zu erstellen, d.h. Listen von Verarbeitungsaktivitäten, die immer eine DSFA erfordern.

Eine vollständige Auflistung der Blacklists der europäischen Datenschutzbehörden finden Sie hier: <https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/>




Über ownCloud

ownCloud ist der Open-Source-Marktführer für Content Collaboration weltweit. Nutzer können von jedem Gerät und überall auf der Welt sicher auf Daten zugreifen und diese austauschen. Mit mehr als 200.000 Installationen und 50 Millionen Nutzern bietet ownCloud Organisationen ein modernes Kollaborationserlebnis und steigert so die Produktivität, ohne die Sicherheit zu beeinträchtigen. Gleichzeitig bietet ownCloud volle Kontrolle und Transparenz bei der Verwaltung sensibler Daten.

Wenn Sie sich über die neuesten Entwicklungen rund um ownCloud auf dem Laufenden halten möchten, besuchen Sie <https://owncloud.com/de/newsroom> oder folgen Sie uns auf Twitter unter [@ownCloud](#).

ownCloud GmbH
Rathsbergstr. 17
90411 Nürnberg
Germany

Kontakt:
owncloud.com/de/kontakt
Telefon: +49 911 14888690
owncloud.com/de

 [@ownCloud](#)
 facebook.com/owncloud
 linkedin.com/company/owncloud