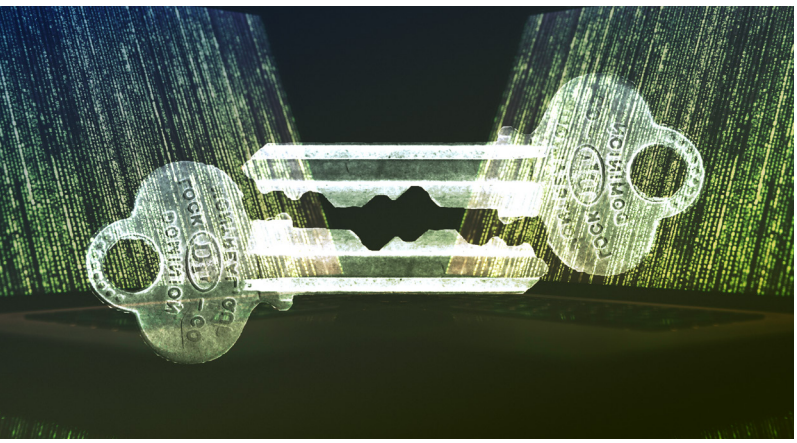
ownCloud
STORE. SHARE. WORK.

Richtlinien zum Datenschutz und Datengeheimnis einhalten

Verschlüsselung in ownCloud

Einführung

Datenschutz ist heute wichtiger denn je. Die seit Mai 2018 geltende Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) und ähnliche Bestimmungen anderer Länder haben das Thema in den Blickpunkt gerückt. Gemäß der Verordnung und den nationalen Bestimmungen, die sich daraus ableiten, müssen datenverarbeitende Organisationen sämtliche personenbezogenen Daten mit Maßnahmen schützen, die dem Stand der Technik entsprechen. Personenbezogene Daten dürfen nicht an die Öffentlichkeit gelangen. Kommt ein Unternehmen seiner Pflicht zum Schutz dieser Daten nicht nach, drohen ihm rechtliche Konsequenzen, Bußgelder oder Imageschäden.



Zur Wahrung des Datengeheimnisses müssen hingegen alle Daten geschützt werden, die für ein Unternehmen oder für bestimmte Personen von Bedeutung sind. Generell kann es für Unternehmen wichtig sein, dass bestimmte Daten nicht offengelegt werden. Vielfach sehen Vertraulichkeitsvereinbarungen und ähnliche Verträge vor, dass beim Umgang mit internen Unternehmensdaten besondere Schutzmaßnahmen zu ergreifen sind.

Datenschutz im Sinne der EU-DSGVO lässt sich durch eine Kombination physischer und organisatorischer Schutzmechanismen erreichen. Physische Schutzvorkehrungen sorgen dafür, dass sich Unbefugte keinen Zugang zu Ihrem Rechenzentrum und Ihren Servern verschaffen können. Organisatorische Schutzmaßnahmen gewährleisten, dass Administratoren über die nötigen Kenntnisse verfügen sowie alle Aktivitäten protokolliert werden und nachprüfbar sind. Meist reichen diese beiden Schutzebenen zur Einhaltung der DSGVO vollkommen aus.

Beim Datengeheimnis verhält es sich anders. In ownCloud sind Daten prinzipiell klar zwischen den Nutzern getrennt. Werden Dateien nicht mit einem anderen Nutzer geteilt, so kann dieser unter keinen Umständen darauf zugreifen. Richtlinien sorgen über die ownCloud File Firewall oder die ownCloud-Erweiterung zur Klassifizierung von Dokumenten dafür, dass bestimmte Dateien nicht ausgetauscht und nicht auf bestimmte Weise abgerufen werden dürfen. Doch auch wenn solche Richtlinien definiert wurden, kann der Systemadministrator nach wie vor alle Daten abrufen, auf die ownCloud Zugriff hat. Um den Zugriff des Systemadministrators zu verhindern, müssen die Daten verschlüsselt werden.

Drei Ebenen der Verschlüsselung

ownCloud bietet eine Reihe von Mechanismen zur Gewährleistung des Datenschutzes und des Datengeheimnisses in Unternehmen. Sowohl für den Datenschutz als auch für das Datengeheimnis kann Verschlüsselung von Vorteil sein. In diesem Whitepaper werden die verschiedenen Verschlüsselungsmöglichkeiten von ownCloud vorgestellt. Es wird außerdem erläutert, wie Sie mithilfe dieser Optionen den Datenschutz und das Datengeheimnis auf Ihrer ownCloud-Plattform für die gemeinsame Bearbeitung von Inhalten gewährleisten.

Sowohl hinsichtlich des Datenschutzes als auch des Datengeheimnisses, kann Verschlüsselung eine unbedingte Pflicht, ein hilfreiches Tool oder sogar eine umständliche Vorgehensweise sein. In einer ownCloud-Umgebung können Daten auf drei Ebenen verschlüsselt werden: bei der Übertragung, bei der Speicherung und auf dem Endgerät. Die letzte Option wird auch als Ende-zu-Ende-Verschlüsselung bezeichnet.

1. Verschlüsselung bei der Übertragung

ownCloud unterstützt standardmäßig die Verschlüsselung bei der Übertragung. Hierzu wird HTTPS mit den neuesten TLS-Protokollen in allen unterstützten Browsern und Clients eingesetzt. Dasselbe gilt für sämtliche Verbindungen zu den Speicher-, Verzeichnis- und Authentifizierungsservern oder zu den unterstützten Diensten zur kollaborativen Bearbeitung von Office-Dokumenten. Die Verschlüsselung bei der Übertragung ist gemäß DSGVO zwingende Voraussetzung für einen angemessenen Datenschutz und entspricht laut verschiedenen Gerichtsurteilen dem Stand der Technik. Sie ist außerdem zwingende Voraussetzung für die Wahrung des Datengeheimnisses.

2a. Verschlüsselung bei der Speicherung

Verschlüsselung bei der Speicherung bedeutet, dass alle Dateien vom ownCloud-Anwendungsserver vor ihrer Speicherung auf dem Speichersystem verschlüsselt werden. Hierfür verwendet ownCloud eine Verschlüsselungsmethode, die auf einem Hauptschlüssel basiert und unter allen Dateisystemen unterstützt wird.

Für S3-Objektspeicher wird die native S3-Verschlüsselung empfohlen. Die Verschlüsselung mit einem Hauptschlüssel sorgt dafür, dass Dateien nicht von den Speichersystemen ausgelesen werden können. Sie werden mit einem Dateischlüssel verschlüsselt, der wiederum mit dem Hauptschlüssel verschlüsselt wird.

Da sich der Hauptschlüssel auf dem Speichersystem befindet, kann der Systemadministrator Dateien durch die Kombination des Dateischlüssels mit dem Hauptschlüssel entschlüsseln. Mit dieser Form der Verschlüsselung lassen sich bei unbefugten Zugriffen auf die Speichersysteme oder auch beim Diebstahl von Festplatten Verstöße gegen das Datengeheimnis vermeiden.

2b. Verschlüsselung bei der Speicherung mit Hauptschlüssel im Hardware-Sicherheitsmodul (HSM)

Um die Entschlüsselung von Dateien durch den Systemadministrator zu verhindern, bietet ownCloud die Möglichkeit, den Hauptschlüssel in einem Hardware-Sicherheitsmodul (HSM) zu hinterlegen. Der Dateischlüssel wird folglich an das HSM gesendet und dort mit einem internen Prozess der ownCloud-Anwendung entschlüsselt. Solange die Integrität des ownCloud-Anwendungsservers gewahrt bleibt, kann der Systemadministrator den Inhalt der Datei nicht auslesen.

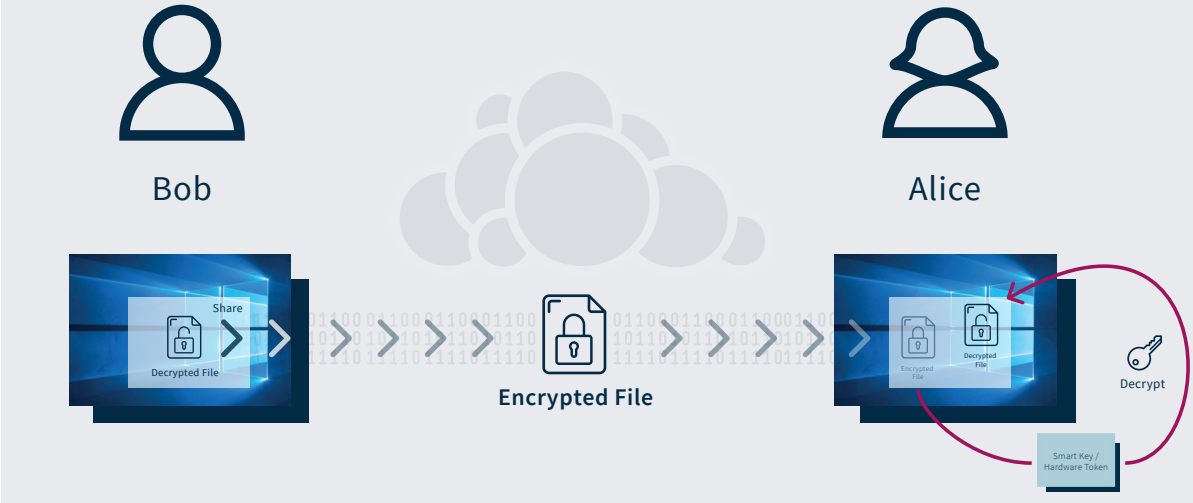
Da Dateinamen aus praktischen Gründen nicht verschlüsselt werden können, sollten sie keine Geheimnisse enthalten. Dadurch bleibt das Datengeheimnis gewahrt, sofern Sie mithilfe entsprechender organisatorischer Maßnahmen in der Lage sind, böswilliges Verhalten zu erkennen und zu unterbinden.

Ein HSM, auf dem der Hauptschlüssel hinterlegt ist, reagiert ausschließlich auf Anforderungen der ownCloud-Anwendung. Hardware-Sicherheitsmodule sind inzwischen auch als Software, Appliance-Lösungen oder kleine Hardware-Dongles erhältlich, die über einen USB-Anschluss mit dem System verbunden werden können. ownCloud unterstützt zertifizierte Hardwaresicherheitsmodule über PKCS 11.

Die oben beschriebenen Lösungen für die Verschlüsselung bei der Speicherung sind im Hinblick auf die Performance mit einem klaren Nachteil verbunden: Für jeden Verschlüsselungsvorgang werden zusätzliche Arbeitsschritte benötigt, die ownCloud ausbremsen. Werden 20.000 Dateien mit einem anderen Nutzer ausgetauscht, müssen zahlreiche Schlüssel im System hinterlegt werden. Außerdem müssen Dateischlüssel verschlüsselt und entschlüsselt werden. Für jede Datei muss hierzu das HSM angesteuert werden. In diesem Fall kann entweder eine zweite ownCloud-Instanz zur Speicherung aller Daten installiert werden, die besondere Schutzmaßnahmen erfordern, oder es wird eine Ende-zu-Ende-Verschlüsselungslösung eingesetzt.

3. Ende-zu-Ende-Verschlüsselung

Wenn Sie absolut sicher sein möchten, dass weder Systemadministratoren noch sonstige Personen auf verschlüsselte Daten zugreifen können, kommt nur eine Lösung mit Ende-zu-Ende-Verschlüsselung infrage. Eine solche Lösung ermöglicht eine optimale Wahrung des Datengeheimnisses und zugleich optimalen Datenschutz. Diese Verschlüsselungsmethode bringt ebenfalls eine Reihe von Nachteilen mit sich: Die Nutzer müssen das Datengeheimnis bzw. die Datenschutzanforderungen der Dateien in jedem einzelnen Ordner



Die Ende-zu-Ende-Verschlüsselung mit Key-Service wird höchsten Anforderungen an das Datengeheimnis und den Datenschutz gerecht.

berücksichtigen, auf der Client-Seite kommt es zu Performance-Einbußen, und der Systemadministrator kann keine Daten für die Nutzer wiederherstellen. Beim Verlust des privaten Schlüssels lassen sich die Daten nicht auf andere Weise wieder entschlüsseln.

ownCloud bietet ein Plug-in für die Ende-zu-Ende-Verschlüsselung an. Das Plug-in ist als Subscription ab 1.000 EUR/Jahr für bis zu 50 Nutzer erhältlich. Wird das Plug-in für einen Nutzer aktiviert, kann er damit leere Ordner verschlüsseln. Durch Sharing können weitere Nutzer eingeladen werden.

Der Besitzer kann bei jeder hochgeladenen Datei sehen, an wie viele und welche Nutzer die Datei gesendet wurde. Vor der Übertragung auf den Server wird die Datei im Browser mit einem JavaScript-Plug-in verschlüsselt, welches sicher an den Browser des Nutzers übertragen wird. Die Verschlüsselung erfolgt mit öffentlichen Schlüsseln, die vom Server abgerufen werden. Auch die Entschlüsselung findet im Browser statt. Hierzu muss der private Schlüssel im Browser des Empfängers hinterlegt sein.

Für größtmögliche Sicherheit bietet ownCloud einen zusätzlichen Key-Service an. Damit kann der private Schlüssel außerhalb des Browsers hinterlegt werden, unter anderem auch in Form eines hardwarebasierten Schlüssels. Dieser sorgt dafür, dass der private Schlüssel auch dem Nutzer nicht bekannt ist, sondern ausschließlich auf dem Hardwaregerät hinterlegt ist.

Bei aktivierter Ende-zu-Ende-Verschlüsselung können Dateien nicht gemeinsam bearbeitet und auch keine serverseitigen Funktionen wie die Überprüfung auf Viren genutzt werden. Da die Lösung jedoch im Browser implementiert wird, ist sie äußerst praktisch, lässt sich einfach nutzen und erfordert keine zusätzliche Software.

Die Rolle des Outlook-Plugins bei der Verschlüsselung

Dateien werden nach wie vor hauptsächlich per E-Mail ausgetauscht, auch wenn Anhänge in der Regel nicht verschlüsselt werden. Das Outlook Plug-in von ownCloud ermöglicht auch ein sicheres Versenden von E-Mail-Anhängen. Anhänge werden automatisch durch Links zu den entsprechenden Dateien in ownCloud ersetzt. Diese Links können durch ein Kennwort geschützt werden.

In Kombination mit dem ownCloud End-to-End Encryption Plug-in werden sämtliche Anhänge mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.

Ausnahme: Gesundheitsdaten nach Artikel 9 Absatz 2.h in Verbindung mit Absatz 3 DSGVO

Wenn Ihr Unternehmen Gesundheitsdaten verarbeitet, müssen Sie entweder die Speicherverschlüsselung mit Hauptschlüssel im HSM anwenden, eine Ende-zu-Ende-Verschlüsselungsmethode verwenden oder sicherstellen, dass Ihre Systemadministratoren nach geltendem Recht der Geheimhaltungspflicht unterliegen.

Zusammenfassung

Mit der Lösung von ownCloud lassen sich alle Herausforderungen im Zusammenhang mit dem Datenschutz und der Wahrung des Datengeheimnisses bewältigen. Sprechen Sie mit uns über Ihre konkreten Anforderungen, etwa die Angriffsvektoren, vor denen Sie sich schützen möchten. Eine ownCloud-Installation mit den richtigen Add-ons bietet Unternehmen jeder Größe höchste Sicherheit auch für hochsensible Daten.

Wenn Sie weitere Informationen wünschen, besuchen Sie auch unsere Website oder setzen Sie sich mit uns in Verbindung.

ownCloud GmbH
Rathsbergstr. 17
90411 Nürnberg
Germany

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

@ownCloud
facebook.com/owncloud
linkedin.com/company/owncloud