Bundesamt
für Sicherheit in der
Informationstechnik

Betrieb und Sicherheit von ownCloud

Danksagung

Wir danken Christoph Puppe von der HiSolutions AG für die Erstellung eines Entwurfs dieser Publikation und Holger Dyroff von ownCloud GmbH für die hilfreichen Kommentare.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de/cloud

Inhaltsverzeichnis

1 Einleitung

ownCloud ist eine Webanwendung, die es ermöglicht Dateien innerhalb einer Organisation und auch nach extern zu übertragen. Sie ist in PHP geschrieben und als Open-Source oder auch als kommerzielle Version mit Wartungsvertrag erhältlich. Mit ownCloud stehen den Nutzern die Vorteile des einfachen Verteilens und gemeinsam Bearbeitens zur Verfügung wobei die Kontrolle über die Daten in der eigenen Hand verbleibt.

Wer heute seinen Benutzern eine komfortable Arbeitsumgebung bieten möchte, sieht sich einer großen Auswahl an Werkzeugen und Produkten gegenüber gestellt. Der klassische Fileserver ist zwar in jeder IT-Landschaft noch Standard, aber die Benutzer fordern komfortablere und dynamischere Wege, Daten auszutauschen. Die eigenen Benutzer sind mobiler, die Daten dementsprechend auch. Eine Datei, die ein Benutzer eben noch auf dem Notebook bearbeitete, will ein anderer Benutzer im nächsten Moment auf einem Tablet anzeigen. Auch die Zusammenarbeit mit Personen außerhalb der eigenen Organisation nimmt stetig zu.

Dieser Dynamik Rechnung zu tragen ist eine nicht unerhebliche Herausforderung für den modernen IT-Betrieb. Neben der Produktivität ist auch die Sicherheit der Daten vor Verlust, Veränderung und Nicht-Verfügbarkeit zu beachten. Der Datenschutz ist zu bedenken, wie auch die Integration der neuen Werkzeuge in die bestehenden Prozesse. Besonders die Verwaltung der Benutzer ist hier in den Fokus gerückt, denn wo früher eine Liste der Mitarbeiter ausreichte, sind heute teilweise sehr unterschiedliche Benutzergruppen zu beachten. In den meisten Fällen sind dies externe Mitarbeiter, Kunden, Partner und Mitarbeiter von Organisationen, mit denen eine Kooperation besteht.

Daten zu bearbeiten und zu teilen innerhalb und außerhalb der eigenen Organisation ist auf vielen Wegen möglich. Viele Angebote sind als Cloud-Dienst realisiert. Die Verteilung der Daten an die Empfänger übernimmt dabei eine fremde Organisation, die über das Internet für alle Beteiligten erreichbar ist. So praktisch dies auch ist, so geht doch die Hoheit über die Daten verloren, denn sie werden bei diesen Angeboten auf den Servern des Anbieters gespeichert. Diese Server stehen bei den großen Anbietern weltweit verteilt und es kann nicht immer sichergestellt werden, dass sie z.B. nur innerhalb des Geltungsbereichs des Europäischen Datenschutzes verarbeitet werden.

1.1 Zielgruppe

Das Ziel dieses Dokuments ist es, interessierten IT-Verantwortlichen einen Überblick über die Möglichkeiten, Sicherheitsmaßnahmen und Einschränkungen für den Betrieb von ownCloud zu geben und den dazu gehörigen Entscheidungsprozess zu unterstützen.

Es richtet sich an Personen, die

- bereits ein Mindestmaß an Kenntnissen in Informationssicherheit haben, und
- eine Entscheidungsvorlage für den Einsatz eines Sharing-Dienstes erarbeiten sollen.

1.2 Abgrenzung

Dieses Dokument ist keine Checkliste für Sicherheitsmaßnahmen, sondern verweist, wo erforderlich, auf weiter gehende Dokumente. Betrachtet wird dabei ein Einsatz in einer Umgebung für den normalen Schutzbedarf. Maßnahmen für Umgebungen mit hohem Schutzbedarf sind, soweit möglich, mit aufgezeigt. Nicht enthalten sind Maßnahmen für sehr hohen Schutzbedarf oder weitergehender Anforderungen (wie etwa Verschlusssachen) an die Sicherheit der verarbeiten Daten.

Dieses Papier soll Verständnis für die Gefährdungen beim Betrieb eines Sharing-Dienstes und die entsprechenden Sicherheitsmaßnahmen aufzeigen. Es unterstützt, aber es ersetzt damit nicht die Erstellung eines Sicherheitskonzepts oder einer Risikoanalyse.

2 Übersicht zu ownCloud

Über die Anwendung können Mitarbeiter Dateien untereinander austauschen oder Dateien an Personen außerhalb der eigenen Organisation übertragen oder von diesen empfangen. Ein typischer Anwendungsfall wäre ein Dienstleister, dem Mitarbeiter größere Mengen an Daten übergeben. Beispielsweise eine Werbeagentur, die Druckvorlagen erhalten soll. Oder ein freischaffender Fotograf kann dort die im Auftrag erstellten Fotos hochladen. Ein anderes rein internes Szenario wäre der Abgleich von Dateien zwischen dem Büro-Arbeitsplatz und mobilen Geräten. Da ownCloud über die Clients Verzeichnisse synchronisiert, reicht es aus, auf dem PC die Daten in dieses Verzeichnis zu legen und der Client auf dem Mobilgerät kopiert sie automatisch.

Als Webanwendung ist ownCloud auf allen gängigen Webservern mit PHP-Unterstützung lauffähig und kann leicht in bestehende Netzwerk- und Verwaltungsinfrastrukturen integriert werden. Hierzu unterstützt das System die Anbindung an Verzeichnisdienste mittels LDAP oder Shibboleth und ist neben der lokalen Datenhaltung auch in der Lage, vorhandene Netzwerkspeicher und -freigaben zu nutzen. Für die Konfiguration nutzt ownCloud eine Datenbank, wobei es auch hier die gängigen Produkte (wie z.B. Oracle, MySQL und PostgreSQL) unterstützt.

Neben der Kern-Funktionalität des Dateiaustausches, bietet ownCloud in der OpenSource Edition die Synchronisation von Kalendern und Adressbüchern. Da dies in den meisten IT-Landschaften bereits durch die Mail-Anwendung abgedeckt wird, geht dieses Dokument auf diese Funktionen nicht näher ein. Auch der Hersteller geht davon aus, dass überwiegend Privatpersonen diese Funktionen nutzen und sie für professionell aufgestellte Organisationen keinen Mehrwert bieten. Deshalb sind diese in der kommerziellen Version nicht enthalten. Auf die Unterschiede der angebotenen Editionen wird weiter unten noch genauer eingegangen.

Neben den Basisfunktionen können Apps ownCloud um zusätzliche Funktionalitäten erweitern.

Für Anwender der Community Version gibt es eine Webseite mit einem Hilfe-Forum. Zahlende Kunden erhalten innerhalb ihres Wartungsvertrages Unterstützung. Die Dokumentation ist im Web verfügbar[1], wenn auch nur auf englisch. Dort finden sich auch Anleitungen für die Absicherung als ständig erweiterter Hardeningguide[2] oder als Übersicht der Sicherheitsfunktionen mit Abwägungen[3].

2.1 Basisfunktionen

Für den Benutzer stellt sich ownCloud als eine Weboberfläche dar, die ihm nach erfolgter Anmeldung eine Sicht auf die verfügbaren Dateien, abgelegt in Verzeichnissen bietet. Der Benutzer kann selbst Daten einstellen oder herunterladen. Die Voreinstellung regelt den Zugriff per Home-Directory und der Nutzer definiert welche Personen auf welche Verzeichnisse zugreifen dürfen. Benutzer können, sofern ihnen das gestattet ist, auch selbst Verzeichnisse anlegen, allerdings werden diese gelöscht, wenn der Benutzer gelöscht wird, daher wird es nicht empfohlen dies zu gestatten bzw. ein Backup seitens des Administrators zu veranlassen, bevor ein Benutzer gelöscht wird.

Neben dem Zugang über die Weboberfläche bietet ownCloud auch an, die Dateien über webDAV oder einen eigenen Client auf Windows, Linux, MAC OS, Android oder iOS zu übertragen und automatisch zu synchronisieren.

ownCloud kann Inhalte mittels Verweise indirekt einbinden. Per Verweis eingebundene Verzeichnisse und Dateien erscheinen dem Benutzer wie lokale Datenhaltung, aber die Daten liegen auf dem Server des jeweiligen Sharing-Dienstes. ownCloud agiert als Proxy.

1 https://doc.owncloud.org/
2 https://doc.owncloud.org/server/8.1/admin_manual/configuration_server/hardening.html
3 https://owncloud.com/wp-content/uploads/2014/10/WP-Optimizing-ownCloud-Security-EN.pdf

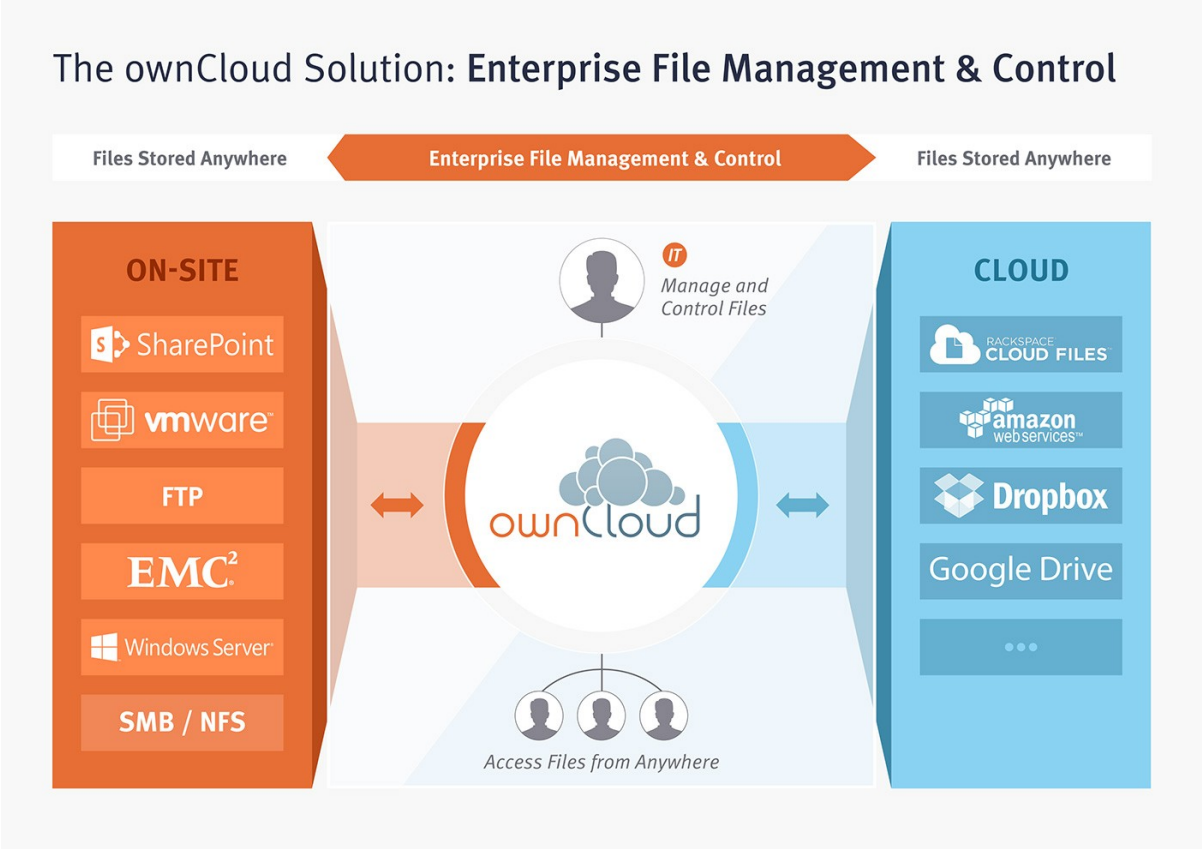

Abbildung 1: Anbindung ownCloud intern und extern, Quelle: https://owncloud.com/owncloud-overview/ Mit freundlicher Genehmigung durch den Rechteinhaber.

Nach dem gleichen Prinzip der Verweise funktioniert auch die Einbettung von weiteren Datenquellen in die ownCloud. In Abbildung 1 ist eine Übersicht der möglichen Anbindungen zu sehen. Der Administrator und auch die Benutzer können Verweise auf Verzeichnisse oder Dateien von Windows-Freigaben, SharePoint-Listen, Amazon S3, Google Drive, Dropbox, Jive, webDAV, S/FTP und OpenStack Object Storage anlegen. Der Benutzer sieht diese dann wie auch die lokale Datenhaltung auf Festplatten oder Speichernetzen und kann auch sein Arbeitsgerät dagegen synchronisieren.

Der IT-Betrieb kann daher mit ownCloud diverse bereits bestehende Angebote in einer Oberfläche zusammenfassen und die Daten mit einer Anwendung auf den Arbeitsgeräten anbieten. Die für die Datensynchronisation erforderliche Anwendung steht für die Betriebssysteme Windows, Linux, Android und iOS zur Verfügung. Sollten sich Daten ändern, kann ownCloud die Benutzer auch per Mail informieren, damit diese sich verbinden und die neuen Versionen der Dateien herunterladen oder automatisch synchronisieren können.

Auch externe Nutzer können diese Plattform nutzen und auf die für sie bereit gestellten Daten zugreifen.

Um die Sicherheit der Daten vor unbefugter Veränderung, Einsichtname oder Verlust zu schützen, bietet ownCloud einige Sicherheitsmaßnahmen. Benutzer werden gemäß ihrer Rolle in Gruppen organisiert und die Zugriffsrechte über die Gruppen eingestellt. Der Dienst kann die Daten auf externen Speichern verschlüsseln und die IT-Administration kann Regeln einstellen, welche Daten der Dienst über welche Verweise transportieren darf. Auch werden alle Zugriffe und Veränderungen protokolliert und wenn gewünscht auch Versionen der Dateien angelegt, so dass die Veränderungen auch rückgängig zu machen sind.

Die Authentifizierung ist bei einem Sharing-Dienst ein besonderes kritischer Punkt, denn nur wenn der Dienst die Benutzer zweifelsfrei und ohne manuelle Aufwände bei der Einrichtung identifiziert, ist Sicherheit vor unbefugten Handlungen möglich. ownCloud verbindet sich dazu neben der lokalen

Benutzerkontenverwaltung mit händisch eingerichteten Benutzern auch mit den gängigen Verzeichnisdiensten. In der aktuellen Version 8 stehen dabei LDAP, IMAP, FTP, SMB, HTTP Basic Authentication und SAML 2.0/ Shibboleth zur Verfügung.

2.2 Neu in Version 8.1

Im Juli 2015 hat ownCloud die Version 8.1 vorgestellt, die neben Verbesserungen der Performance und neuen Funktionen, aus IT-Sicherheitssicht relevante Änderungen beim Schlüsselmanagement bei verschlüsselten Daten enthält. So ist es nun möglich die Schlüssel in einem externen System zu verwalten. Damit kann die Verschlüsselung auch bei Single-Sign-On mit Shibboleth die Dateien sichern. Damit integriert sich ownCloud besser in vorhandene Infrastrukturen. Dies ermöglicht zwar nun (im Unterschied zur Version 8.0) eine verschlüsselte Dateiablage mit einem Zweifaktor-Schutz, jedoch sind die Schlüssel in diesem Fall bei einer externen Anwendung und dort wiederum nicht verschlüsselt, so dass privilegierte Nutzer Zugriff darauf haben können. Gleichzeitig ist die externe Schlüsselverwaltung ein lukratives Ziel für Angriffe.

Eine weitere wichtige Neuerung ist die Verwaltung von Identitäten in verteilten Umgebungen, die Unterstützung der sogenannten federated ID ist in dieser Version verbessert. Benutzer können die Identitäten von anderen ownCloud Servern in ihren Adressbüchern hinterlegen und stehen auch in Dialogen zum Teilen von Dokumenten zur Verfügung.

Andere Detailverbesserungen betreffen die Anbindung externer Speicher. So kann jetzt auch ein SSH-Schlüssel bei SFTP die Authentifizierung übernehmen. Die Einstellung für Vertrauenswürde Domains, von denen ownCloud annimmt, ist nun ein Pflichtfeld. Fehlerhafte Konfigurationen, wo Server zu weit offen waren, verhindert ownCloud so. In früheren Versionen wurde bei Verwendung eines reverse Proxy in der Protokollierung von Zugriffen die IP des Proxy eingetragen. In 8.1 wird nun die IP des eigentlichen Clients aus den Header ausgelesen und im Logfile eingetragen. Die Sitzungs-Marker (Session IDs) kann nun der Apache mit dem Modul mod_unique_id erstellen. Dies bringt eine erhöhte Sicherheit, da das Modul Marker erzeugt, die sich nicht wiederholen und eindeutig sind. Bugs im Quellcode hat das ownCloud Team genauso bereinigt, wie auch Content-Security-Policy eingebaut.

Andere Funktionen sind, um die Sicherheit zu erhöhen, in ownCloud nicht mehr enthalten. Ein Download von Dateien vom ownCloud Server selbst über den „From Link“ führte dazu, dass der Server von seiner IP aus teilweise Zugriff auf Daten hatte, die der Benutzer nicht hätte erhalten dürfen. Die „From Link“ Downloads sind nicht mehr möglich in 8.1.

Zusammen mit der neuen „Tipps und Tricks“ Sektion im Handbuch mit Hinweisen auf die sichere Konfiguration von ownCloud sind die vielen kleinen Verbesserungen und die neu geschriebene Schlüsselverwaltung ein eindeutiger Schritt in die richtige Richtung. Leider wurde in der 8.1 ein gravierender Fehler eingebaut, daher ist die Empfehlung direkt die 8.1.1 oder neuere Versionen einzusetzen.

2.3 Vergleich Community und Enterprise Edition

Bis zur Version 7 war ownCloud in zwei Editionen erhältlich. Die kostenfreie Community Edition und die kostenpflichtige Enterprise Edition. Seit der im Februar 2015 erschienenen Version 8 stellt ownCloud 8 Server (bislang unter dem Namen ownCloud Community Edition bekannt) grundlegende Funktionen für Filesync und -share als kostenfreie Community Version bereit. Diese umfassen verschiedene Server-Apps für die Verwaltung und Kontrolle von Filesharing-Aktivitäten, Virenschutz, Verschlüsselung, Unterstützung von externem Speicher, LDAP/AD, Federated Cloud Sharing, Provisioning, Versionskontrolle und mobile Apps, die über den App Store von ownCloud erhältlich sind. Neu ist, dass Kunden seit Februar mit der Standard Subscription kostenpflichtigen Support für ownCloud Server erhalten, die unter AGPLv3 lizenziert wird.

Support für die kostenpflichtige ownCloud 8 Enterprise Edition wird im Rahmen der Enterprise Subscription angeboten (ownCloud Commercial License).

Neben dem Funktionsumfang von ownCloud 8 Server verfügt die kostenpflichtige ownCloud 8 Enterprise Edition über erweiterte Funktionen und speziell auf die Anforderungen von Unternehmen zugeschnittene Apps.

Dies sind:

- SharePoint-Anbindung
- Anbindung von Windows-Freigaben inkl. Heimverzeichnisse
- File Firewall – Regeln für die Einschränkung der Verteilung auf Basis von Dateieigenschaften
- Protokollierung der Benutzeraktivitäten mit Auswertungen

Kalender und die Adressbücher sind optional bei beiden Versionen ohne Support möglich.

Eine aktuelle Tabelle der Funktionalitäten beider Versionen sind hier (https://owncloud.com/de/owncloud-server-or-enterprise-edition/) zu finden.

2.4 Erweiterung mit Apps

Apps sind Programme in PHP, die den Funktionsumfang von ownCloud erweitern. Sie nutzen dafür die vom Produkt bereitgestellten Schnittstellen. Die Apps sind dabei nicht eingeschränkt und können jeden Aspekt des Sharing-Dienstes erweitern oder verändern.

Es ist zwischen den vom Hersteller und den von sonstigen Entwicklern bereitgestellten zu unterscheiden. Der Hersteller bietet für die nicht von ihm entwickelten Erweiterungen keinen Support an, unterstützt die Community jedoch durch die Bereitstellung eines Marktplatzes, auf dem zum jetzigen Zeitpunkt (März 2015) etwas über 200 Apps gelistet sind. Dank Bewertungssystem sind beliebte und gut funktionierende Apps schnell zu finden.

Die Apps mit den besten Bewertung auf dem Marktplatz waren aktuell (März 2015):

- ownNote – Notizen Editor mit WYSIWIG
- Shorty – Kurz URL Service um aus langen URLs eindeutige kurze zu erzeugen
- Tasks – Aufgabenplanung
- Roundcube – WebMail
- Files Move – Kopieren und Verschieben
- Files Tree – Verbesserte Navigation in Verzeichnissen
- Mozilla Sync – Synchronisiert Daten des Firefox (Bookmarks, Passwörter etc.)
- Mobile compatible theme – Eine Anpassung der Oberfläche für Mobile Geräte

Der Betreiber von ownCloud kann natürlich auch durch selbst geschriebene Apps die Funktionen nach eigenen Vorstellungen erweitern und anpassen. Der Hersteller bietet dies auch als kostenpflichtigen Service an. Die API sind offen dokumentiert, es gibt eine Mailingliste für Hilfe und Erfahrungsaustausch.

2.5 Architektur und Betriebsmodelle

ownCloud kann wie jeder Anwendungsdienst in unterschiedlichsten Modellen betrieben werden. Die Bandbreite reicht dabei von einer Installation in einer virtuellen Maschine mit lokaler Datenhaltung für Dateien und Datenbank bis hin zu einer verteilten Anwendung mit hunderten Servern, um parallel große Arbeitslasten zu bewältigen. Neben diesem Betriebsmodell ist es auch möglich, die Server betreiben zu lassen, wobei damit natürlich der große Vorteil der eigenen Hoheit über die Daten aufgeweicht wird.

2.5.1 Architektur

Zum Betrieb von ownCloud ist eine Datenbank, ein Webserver, und ein Datenspeicher erforderlich. Man kann alle drei auf einem System unterbringen oder sie auf verschiedene Server in mehreren Rechenzentren verteilen. Abbildung 2 zeigt eine beispielhafte Architektur, in der alle wichtigen Komponenten redundant ausgelegt sind. ownCloud lässt damit auch Anwendungsfälle mit hoher Verfügbarkeitsanforderung zu.

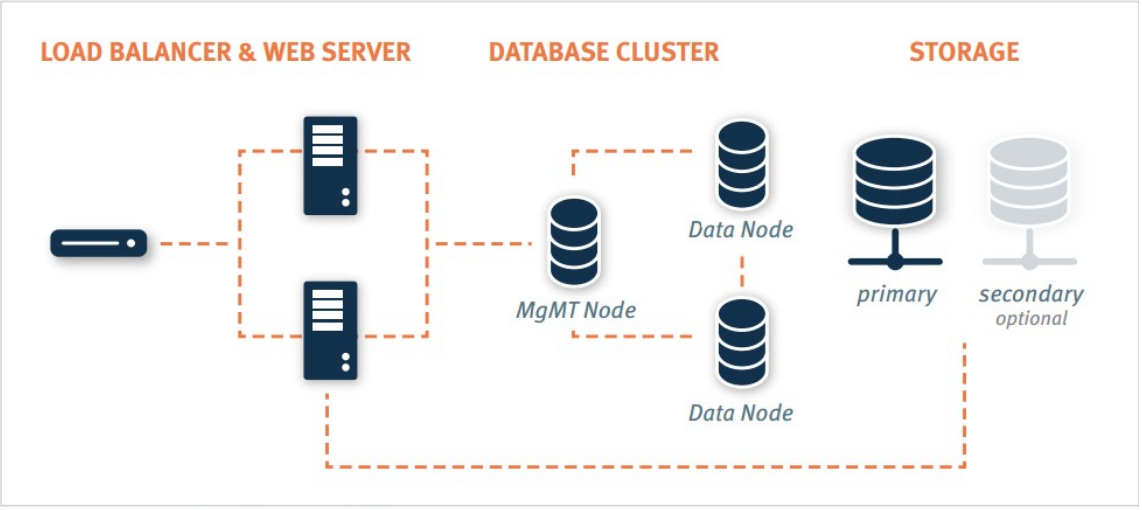

Figure 4: Common ownCloud Deployment Architecture

Abbildung 2: Redundante und verteilte ownCloud Installation.
Quelle: https://owncloud.com/wp-content/uploads/2014/03/oc_architecture_overview.pdf
Mit freundlicher Genehmigung des Rechteinhabers.

2.5.2 Eigenbetrieb

Die am weitest gehende Kontrolle über die Daten behält die Organisation, wenn der komplette Betrieb in den eigenen Räumen und Netzen erfolgt und nur die eigenen Administratoren den Betrieb verantworten. ownCloud ist einfach zu betreiben und benötigt keine besonderen Spezial-Kenntnisse, die über den Betrieb eines Webservers und einer Datenbank hinaus gehen.

In diesem Modell ist die Organisation für die Sicherheit inkl. Schutz aller Sicherheitsziele und Datensicherungen selbst verantwortlich.

2.5.3 Fremdbetrieb

Fremdbetrieb sind alle Betriebsmodelle in denen ein Auftragnehmer die Server betreibt. Das kann in eigenen Räumen und eigenen Netzen sein (sog. on-premise), aber auch der Betrieb der Anwendung in der Lokalität des Auftraggebers (sog. off-premise) ist ein gängiges Modell.

Die Architektur ist unabhängig von der Frage wer die Umgebung betreibt, allerdings sind zusätzliche Netzübergänge für z.B. den Wartungszugang einzuplanen.

2.5.4 Hosting / Housing

Beim Housing und Hosting stehen die Server in den Räumen und im Netz des Auftragnehmers. Sie werden entweder selbst oder vom Auftragnehmer betrieben. Die Architektur kann der Auftraggeber auch hier frei wählen. Wobei viele Dienstleister auch eigene Infrastruktur zur Nutzung anbieten. Dies können Datenspeicher, Datenbanken, Backup und weitere Infrastrukturdienste sein.

2.5.5 ownCloud als Cloud-Dienst

Den Sharing-Dienst beim public Cloud Anbieter zu betreiben ist auf zwei Wegen möglich. Entweder als Software-as-a-Service (SaaS), also Hosting auf einer zumeist virtuellen Instanz, häufig auch mit anderen Kunden auf den gleichen Systemen. Hierbei wird vom Anbieter der Dienst bereits vorinstalliert und es gibt keinen Zugang zum Betriebssystem. Zahlreiche Anbieter bieten dies an.

Auch in einem Infrastruktur as a Service (IaaS) Dienst kann ownCloud installiert werden. Der Anbieter stellt einen virtuellen Server bereit, zumeist inklusive Betriebssystem. Installation und Betrieb erfolgt durch die Organisation selbst.

Auf der Webseite von ownCloud ist eine Liste mit Anbietern. Die von ownCloud unterstützten sind unter der Bezeichung "Supported Providers" zu finden.

2.6 Anbindung an interne und externe Dienste

ownCloud als Dienst bietet bereits einige Funktionen, allerdings erst eingebunden in die bereits vorhandenen Dienste und Anwendung entfaltet es seine volle Leistung. Es stehen bereits sehr viele Schnittstellen bereit und Apps können die Fehlenden hinzufügen.

2.6.1 Authentifizierung

Für die Authentifizierung gibt es eine lokale Benutzerverwaltung in ownCloud mit Benutzernamen und Passwort. Für jeden Benutzer ist im ownCloud ein Benutzeraccount notwendig. Die eingebaute Verwaltung ist sehr einfach gehalten. Erweiterte Funktionen wie zwei Faktor-Authentifizierung oder die Kontrolle der Passwörter auf Komplexität ist nur über zusätzliche Apps möglich. Eine Besonderheit ist Shibboleth (siehe unten), denn um diesen Dienst anzubinden muss die Shibboleth App von ownCloud benutzt werden.

ownCloud kann beliebige Verzeichnisdienste über LDAP einbinden. Benutzernamen und Zugehörigkeit zu Gruppen sind über LDAP genauso abrufbar, wie Heimatverzeichnisse, Profilbilder, Adressen und weitere Merkmale, sofern der Verzeichnisdienst dies unterstützt. Bei der ersten Anmeldung über einen der Anmeldedienste richtet ownCloud den Benutzeraccount lokal ein.

Neben den im eigenen Verzeichnisdienst geführten Mitarbeitern sind allerdings oft noch weitere Gruppen von Nutzern zu beachten. In vielen Fällen sind dies z.B. die Mitarbeiter einer Partnerorganisation, die Zugriff auf bestimmte interne Ressourcen erhalten sollen. Der früher übliche Weg war, vom Partner eine Liste der Personen zu erhalten und diese manuell einzurichten. Heute setzt sich durch, dass die gemeinsam genutzten Anwendungen die Verzeichnisdienste der Partner dynamisch anbinden. Teilweise wird dafür weiterhin LDAP eingesetzt, allerdings sind neuere Protokolle (z.B. SAML und OAuth2) für diese Art der verteilten Authentifizierung besser geeignet. Auch möchten sich Benutzer nicht an jedem Dienst erneut anmelden, für die Benutzer ist es komfortabler, wenn Dienste ein Single-Sign-On ermöglichen.

ownCloud bietet Single-Sign-On und die Authentifizierung von weiteren Gruppen von Benutzern durch Shibboleth, das für Apache als Modul angeboten wird. Dabei authentifiziert sich ein Benutzer gegen einen Anmeldedienst und erhält ein Security Assertion Markup Language (SAML) Token, das ihn gegenüber der ownCloud ausweist. Jede Gruppe von Nutzern hat dabei oft ihren eigenen Anmeldedienst, der wiederum die Benutzer gegen den Verzeichnisdienst dieser Gruppe authentifiziert. Die ownCloud akzeptiert die Token aller Anmeldedienste, die als vertrauenswürdig hinterlegt sind.

Ein Beispiel sind zwei Organisationen die auf einem ownCloud zusammenarbeiten wollen. Beide richten jeweils einen Anmeldedienst mit Shibboleth ein, der den jeweils eigenen Mitarbeitern – sofern sie ownCloud nutzen dürfen – nach Authentifizierung ein Token erstellt. Mit diesem Token kann sich der Mitarbeiter dann am gemeinsamen Sharing-Dienst anmelden, ohne erneut seinen Benutzernamen oder sein Passwort eingeben zu müssen.

Apps können ownCloud um weitere Authentifizierungsdienste erweitern. Sofern die App für den bereits im Einsatz befindlichen Dienst noch nicht existiert, kann sie auch selbst geschrieben werden.

2.6.2 Speicher

ownCloud speichert die Daten entweder lokal oder verteilt. Es kann alle Arten von lokalen Massenspeichern nutzen, aber auch ein SAN anbinden. Zu beachten ist, dass für die lokale Datenhaltung alle Zugriffe als der Benutzer erfolgen, unter dem der Webserver betrieben wird. Dies gilt allerdings nur für Datenspeicher die per CIFS, SAN, NFS und anderen Methoden im Betriebssystem des Webservers eingebunden sind, der die Anwendung betreibt.

ownCloud kann zudem fast alle gängigen Cloud-Speicher einbinden. Die Freigaben zeigt ownCloud dabei für den Benutzer transparent in der Oberfläche an. Dort stehen sie für den Zugriff über die Web-Oberfläche oder zur Synchronisation mittels der ownClound Anwendung bereit.

Folgende externe Speicher werden von ownCloud unterstützt (Stand März 2015):

- Google Drive
- Amazon S3 und Dienste die das gleiche Protokoll bedienen
- FTP / SFTP
- Swift
- Dropbox
- webDAV
- SharePoint
- SMB (Windows Network Drive)

Die Datenhaltung auf den externen Speichern erfolgt dabei auf Wunsch auch verschlüsselt. Seit der Version 8.1 ist dies auch möglich, wenn Shibboleth die Authentifizierung übernimmt. Damit ist im Unterschied zu Version 8.0 grundsätzlich auch eine Zweifaktor-Authentisierung bei gleichzeitiger Dateiverschlüsselung möglich. Jedoch müssen dazu die Schlüssel aller Nutzer bei Shibboleth unverschlüsselt vorliegen, was ein neues Risiko darstellt. Diese Randbedingung ist bei der Planung zu beachten.

2.6.3 Server zu Server Sharing

Mehrere Instanzen von ownCloud können Administratoren und Benutzer über einen Link miteinander verbinden. Für den Benutzer sind diese Verzeichnisse in der Oberfläche sichtbar wie jeder andere Datenspeicher und er kann sie auch automatisch mit dem Client auf seinem Arbeitsgerät synchronisieren.

2.6.4 Verteilen an Personen ohne Benutzeraccount

Nicht jede Person, die Zugriff auf eine Datei oder Verzeichnis benötigt, hat auch einen Account im ownCloud. Für Zugriffe dieser Art bietet ownCloud – sofern aktiviert – eine Freigabe per Link an. Die Links führen direkt zum freigegebenen Inhalt. Weitere Daten sind darüber nicht verfügbar. Diese Freigaben sind, sofern so eingestellt, nur eine begrenzte Zeit gültig und der freigebende Nutzer kann ein Passwort definieren, das für den Zugriff notwendig ist.

2.6.5 Versionsverwaltung

Bei Veränderungen an bestehenden Dateien kann ownCloud die ehemaligen Versionen weiter vorhalten und ermöglicht die Wiederherstellung. Die Versionierungs-App reguliert alte Versionen, um sicherzustellen,

dass der Speicherplatz im Rahmen bleibt und nie mehr als 50% des verfügbaren Speicherplatzes benötigt wird.

2.6.6 Virenscanner

Mit ownCloud wird ClamAV ausgeliefert, der alle eingestellten Dateien auf Viren untersucht. Seit Version 7 und der Antivirus App sind auch alternative Produkte möglich. Prinzipiell funktionieren alle Produkte, die ownCloud über eine Kommandozeile aufrufen kann. Beispiele für die Anbindung bekannter Produkte liegen leider nicht vor.

2.6.7 Logging und Monitoring

In der kommerziellen Version protokolliert ownCloud seine Aktivitäten entweder direkt in sein Datenverzeichnis auf dem WebServer oder über Syslog.

Zusätzlich stehen auch für die kostenlose Version Apps zur Verfügung, die die Aktionen der Benutzer protokollieren.

3 Gefährdungen

In diesem Dokument soll eine Entscheidungshilfe für oder gegen den Einsatz von ownCloud in der Organisation gegeben werden. Die hier genannten Gefährdungen sind daher nur ein Ausgangspunkt, um sich vor dem Einsatz über die Risiken bewusst zu werden und – sofern gewünscht – eine vollständige Risikoanalyse durchzuführen. Ein Vorgehen für eine Risikoanalyse ist im BSI Standard 100-3 beschrieben.

Je nach Betriebsmodell wirken unterschiedliche Gefährdungen auf die Anwendung. Wobei ein Großteil der Gefährdungen nicht anwendungsspezifisch für ownCloud sind. Wo vorhanden, sind die Gefährdungen aufgezeigt, die auf Sharing-Dienste wie ownCloud oder nur ownCloud wirken. Ein eigener Abschnitt beschäftigt sich mit den für ownCloud originären Gefährdungen, die unabhängig vom Betriebsmodell wirken. Dieser Abschnitt ist, wie auch die anderen einfach auf andere Sharing-Dienste zu übertragen. Sollten mehrere Produkte in Frage kommen, ist es so möglich, die Sicherheitsmerkmale dieser Produkten anhand ihrer Wirksamkeit gegen diese Gefährdungen zu vergleichen.

3.1 Allgemeine Gefährdungen

Die für den Betrieb eingesetzten IT-Systeme unterliegen einer Anzahl von allgemeinen Gefährdungen, die für alle Server und Anwendungen gelten. Diese Gefährdungen werden in den passenden Bausteinen der IT-Grundschutz-Kataloge aufgeführt. Es sind je nach Betriebsmodell dabei unterschiedliche Bausteine zu beachten.

3.1.1 Eigenbetrieb

Der Betrieb von ownCloud unterscheidet sich in der Betrachtung der Gefährdungen nicht vom Betrieb anderer Server. Die für dieses Betriebsmodell relevanten Gefährdungen finden sich in den IT-Grundschutz-Katalogen in den Bausteinen zum RZ- und Server-Betrieb.

Vorrangig zu betrachtende Gefährdungen sind:

- Feuer
- Wasser
- Ausspähen von Informationen / Spionage
- Manipulation von Informationen
- Unbefugtes Eindringen in IT-Systeme
- Unbefugtes Eindringen in Räumlichkeiten

Für eine initiale Betrachtung der Risiken ist der Gefährdungskatalog „G 0 Elementare Gefährdungen“ gut geeignet.

3.1.2 Fremdbetrieb

Sobald man zusätzliche Prozesse, Mitarbeiter und Organisationen in den Betrieb der IT-Systeme involviert, ergeben sich zusätzliche Gefährdungen. Wo im Eigenbetrieb nur die eigenen Mitarbeiter unabsichtlich oder absichtlich Fehler machen, sind durch den Dienstleister nun auch dessen Mitarbeiter in der Lage den sicheren Betrieb zu stören. Auch steigt durch die notwendigen Wartungszugänge das Risiko eines Angriffs durch betriebsfremde Personen. Einerseits weil die Wartungszugänge selbst das Einfallstor für den Angriff sind und auch weil die IT-Systeme und Netze des Dienstleisters für den Angreifer eine Möglichkeit darstellen, auf die eigenen IT-Systeme zuzugreifen.

Neben den technischen Risiken, wird die fehlende Kontrolle über Mitarbeiter, Prozesse und IT-Systeme sowie die Schnittstellen zum Betreiber für die Organisation zum zusätzlichen Risiko.

Vorrangig zu betrachtende Gefährdungen sind:

- Ausfall eines Weitverkehrsnetzes
- Unzulängliche vertragliche Regelungen mit einem externen Dienstleister
- Ungenehmigte Nutzung von externen Dienstleistungen

Für die Risikoanalyse sind die Gefährdungen des IT-Grundschutz Bausteins „B 1.11 Outsourcing“ heranzuziehen.

3.1.3 Housing / Hosting

Der Betrieb der Anwendung in einer nicht von der eigenen Organisation kontrollierten Umgebung führt zu zusätzlichen Risiken. Die Sicherheit des Standortes und auch der dort betriebenen Netze liegt in der Verantwortung des Auftragnehmers und der Auftraggeber hat keinen direkten Einfluss auf die Ausführung. Daher sind auch in diesem Fall die für die Risikoanalyse die Gefährdungen des IT-Grundschutz Bausteins „B 1.11 Outsourcing“ heranzuziehen.

Vorrangig zu betrachtende Gefährdungen sind:

- Ausfall eines Weitverkehrsnetzes
- Unzulängliche vertragliche Regelungen mit einem externen Dienstleister
- Ungenehmigte Nutzung von externen Dienstleistungen

Da in diesem Betriebsmodell die IT-Systeme des Sharing-Dienstes räumlich von den anderen IT-Systemen der Organisation getrennt stehen, ist die Anbindung von internen Datenspeichern und des internen Verzeichnisdienst zusätzlich zu betrachten. Für einen in die internen Dienste eingebundenen Sharing-Dienst müssen Vertrauensstellungen zwischen den entfernten Netzen und dem Netzwerk in den eigenen Standorten aufgebaut werden. Die damit verbundenen Risiken sind erheblich und in der Kosten-Nutzen-Analyse mit zu beachten.

In vielen Fällen wird die Verbindung der beiden Standorte über ein Site-To-Site VPN erfolgen. Für die damit verbundenen Risiken sind für die Risikoanalyse die Gefährdungen des IT-Grundschutz-Katalog Bausteins „B 4.4 VPN“ heranzuziehen.

3.1.4 Betrieb in der Cloud

Beim Betrieb in der Cloud sind alle Gefährdungen, die auch auf den Eigenbetrieb wirken, relevant und es kommen zusätzlich die Gefährdungen des Fremdbetriebs und des Hostings hinzu. Für die Risikoanalyse sind daher die Gefährdungen der IT-Grundschutz Bausteine „B 1.17 Cloud-Nutzung“ und, sofern der ownCloud Server per VPN angebunden wird, auch die Gefährdungen des IT-Grundschutz Bausteins „B 4.4 VPN“, heranzuziehen. Für Anwender, die nicht IT-Grundschutz benutzen ist in der Broschüre „Sichere Cloud-Nutzung“ ein allgemeiner Prozess zur sicheren Cloud-Nutzung beschrieben.

Wie auch bei anderen Formen des Hostings, ist auch bei einem ownCloud als SaaS die Anbindung an interne Ressourcen problematisch, allerdings sind bei klassischen Hosting Angeboten eher eigene Netzbereiche möglich, die man per VPN verknüpft. Ein ownCloud als Dienst hat diese Möglichkeit zumeist nicht, damit ist die Sicherheit der Anbindung hierbei vollständig von der Sicherheit der verwendeten Protokolle zum Datentransport auf Anwendungsebene abhängig, eine zweite Schicht der Sicherheit ist damit nicht möglich.

Nicht nur der ownCloud Server ist in diesem Szenario direkt aus dem Internet erreichbar, sondern auch alle internen IT-Systeme mit denen er Daten austauschen muss, müssen aus dem Internet erreichbar sein. Dies kann umfassen:

- SharePoint
- Verzeichnisdienst
- Dateiserver mit webDAV, S/FTP oder S3

Alle diese IT-Systeme können Software-Schwachstellen und -Fehler enthalten, was in der Risikoanalyse zu berücksichtigen ist. Da die Sharing-Dienste über das Internet erreichbar sind, steigt die Eintrittswahrscheinlichkeit erheblich und daher müssen Gegenmaßnahmen ergriffen werden.

3.2 Spezifische Gefährdungen zu ownCloud

Aus der Anwendung ergeben sich spezifische Gefährdungen, die beim Betrieb eines ownCloud zu beachten sind, unabhängig vom Betriebsmodell. Neben den hier aufgezählten Gefährdungen sind für die Risikoanalyse auch die Gefährdungen des IT-Grundschutz Bausteins „B 5.3 Groupware“ heranzuziehen.

Manche Gefährdungen sind für eine ownCloud Installation besonders zu beachten. Diese sind in den folgenden Abschnitten aufgeführt.

3.2.1 Offenlegung schützenswerter Informationen

Der Sharing-Dienst ermöglicht den Benutzern den Austausch von Dateien mit allen Benutzern des Dienstes. Die Benutzer sind entweder nur Mitarbeiter der eigenen Organisation oder – wie in vielen Installationen üblich – auch die Mitarbeiter anderer Organisationen oder beliebige Personen außerhalb der Organisation. Da die Daten über die ownCloud so die Organisation verlassen können, hat diese Gefährdung eine hohe potentielle Schadenshöhe. Aber auch die Offenlegung der Informationen an unberechtigte Personen innerhalb der eigenen Organisation ist ein zu betrachtendes Risiko.

Dabei ist es unerheblich, ob die Offenlegung eintritt durch eine:

- unabsichtliche Fehlhandlung eines Benutzers,
- absichtliche Fehlhandlung eines Benutzers,
- unabsichtliche Fehlkonfiguration, oder durch
- Fehler in der Software, die alle Daten auf dem ownCloud Server dem Angreifer preisgibt.

3.2.2 Schadprogramme

Über den Austausch von Dateien können die Nutzer auch Schadprogramme an andere Nutzer weitergeben. Wenn sie diese Dateien dann auf Arbeitsgeräte kopieren kann die enthaltene Schadroutine zur Ausführung kommen und das Arbeitsgerät infizieren.

3.2.3 Unberechtigte IT-Nutzung

Nur Benutzer, für die es betrieblich notwendig ist, dürfen auf den Sharing-Dienst zugreifen. Da die Anwendung in vielen Fällen für Mitarbeiter und organisationsfremde erreichbar ist, ist die Verwaltung der Benutzer komplexer als bei Anwendungen, die nur eigene Mitarbeiter zugänglich ist.

Es besteht das Risiko, dass Personen die keine Notwendigkeit zur Nutzung des ownCloud mehr haben, weiterhin als aktive Benutzer in der Anwendung eingetragen sind, sofern die Institution keinen geregelten Prozess zum Austragen von organisationsfremden Personen etabliert hat bzw. diesen Prozess noch nicht auf externe Benutzer ausgeweitet hat.

So sind z. B. Berater und externe Projektmitarbeiter nur für den Zeitraum ihrer Beschäftigung in der Organisation zur Nutzung berechtigt, aber bei Ende des Projektes oder der Beauftragung findet häufig keine Benachrichtigung der Administration über das Ende des berechtigten Nutzung statt. Dieses Risiko ist auch

bei den Mitarbeitern von Partnerorganisationen anzuwenden, da auch hier die Prozesse zwischen Personalverwaltung und Administration des Sharing-Dienstes eventuell nicht gegeben oder nicht zuverlässig sind.

Erschwerend kommt hinzu, dass die Anwendung zumeist über das öffentliche Internet erreichbar ist und die ehemals berechtigte Person weiterhin einfach auf die Anwendung zugreifen kann.

Die Eintrittswahrscheinlichkeit dieser Gefährdung ist sehr hoch und je nach Sensibilität der Daten im Sharing-Dienst, kann die Schadenshöhe auch sehr hoch sein.

4 Sicherheitsmaßnahmen

Die Sicherheit einer Anwendung ist von den Sicherheitsmaßnahmen auf allen IT-Systemen, aber auch denen der Infrastruktur und der Vertrauenswürdigkeit der die Anwendung administrierenden und nutzenden Personen abhängig. Um einen sicheren Betrieb zu gewährleisten sind daher alle Einflussfaktoren zu beachten.

Die hier aufgeführten Maßnahmen sind Empfehlungen für den Betrieb von ownCloud mit einem Schutzbedarf von normal bis hoch nach der Definition des BSI Standards 100-2.

Der BSI-Standard 100-2 definiert drei Schutzklassen:

- "normal" – Die Schadensauswirkungen sind begrenzt und überschaubar.
- "hoch" – Die Schadensauswirkungen können beträchtlich sein.
- "sehr hoch" – Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Der Standard definiert ein Vorgehen, wie aus dem Schutzbedarf der verarbeiteten Daten und dem der unterstützten Prozesse die Schutzklasse jedes Systems, Raums, Netzes und Anwendung hergeleitet wird. Dabei ist auch zu beachten, dass manche dieser Objekte für Daten und Prozesse im Einsatz sind, die unterschiedlichen Schutzbedarf haben. Es wird dabei jeweils der höchste Wert übernommen, das Maximalprinzip. Auch vereinen manche Objekte eine hohe Anzahl von Daten und Prozessunterstützungen in sich, in diesem Fall wird der Schutzbedarf durch den Kumulationseffekt um eine Stufe erhöht.

4.1 Maßnahmen zu ownCloud

Diese Einstellungen verbessern die Sicherheit von ownCloud gegen die genannten Gefährdungen auf Anwendungsebene. Zu beachten ist, dass nicht jede Organisation alle Maßnahmen umsetzen kann und die Gefährdung durch die Maßnahmen nicht verhindert, sondern nur der Eintritt unwahrscheinlicher und / oder die Schadenhöhe geringer wird.

4.1.1 Planung des Betriebs und Absicherungen

Ein Sharing-Dienst ist eine komplexe Anwendung mit technischen und organisatorischen Abhängigkeiten. Die Planung ist mit allen Beteiligten Abteilungen durchzuführen, um schon im Vorfeld die Bedingungen für den Betrieb ausreichend zu klären.

Der Beginn der Planung ist eine Analyse, die die folgenden Fragen klärt:

- Welche Ziele soll der Betrieb der Anwendung erreichen?
- Welche Mengen an Daten und Anfragen sind zu erwarten?
- Welchen Schutzbedarf haben die Daten?
- Welche Abteilungen und Personen dürfen auf die Anwendung zugreifen?
- Welche Verfügbarkeit muss die Anwendung besitzen?
- Welche Kompetenzen sind in der Organisation vorhanden und welche sollen aufgebaut werden?

Die Antworten auf diese Fragen sind Grundlage für die konkrete Planung des Betriebs:

- Welches Betriebsmodell ist zu wählen?
- Auf wie viele Server verteilt sich die Anwendung? Datenbank, Speichersysteme und Web-Frontends, eventuell auch Loadbalancer.

- Ist die Anwendung nur an einem Standort oder verteilt über mehrere Standorte aufgebaut?
- Wird der Zugriff über VPN oder direkt aus dem Internet ermöglicht?
- In welchem Netzsegment werden welche Teile der Anwendung aufgestellt?
- Werden externe Speicher (Amazon, Google, Dropbox etc) angebunden?
- Welche internen Speicher (Windows Shares, SAN, SharePoint etc.) werden eingebunden?
- Welche Gruppen sind notwendig, um allen Nutzern alle Daten, die sie benötigen, aber auch nur diese bereit zu stellen?
- Welche zusätzlichen Apps werden benötigt?
- Sollen Anpassungen erfolgen, die z.B. in einer selbst entwickelten App münden?

Die Ergebnisse sind in einem Anforderungskatalog zu dokumentieren, der auch die notwendigen Sicherheitsmaßnahmen enthält. Die Administration oder der Dienstleister ist zur Umsetzung der geplanten Sicherheitsmaßnahmen zu verpflichten und die Umsetzung ist zu kontrollieren.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in den folgenden Maßnahmen des IT-Grundschutzes:

- M 2.315 Planung des Servereinsatzes
- M 2.454 Planung des sicheren Einsatzes von Groupware-Systemen

4.1.2 Richtlinien zu Nutzung und Sicherheit

Aus den definierten Anforderungen an die Sicherheit und dem geplanten Einsatzzweck ist eine Richtlinie abzuleiten, die für alle Nutzer und Administratoren zugänglich ist. In dieser Richtlinie sind die Regeln für die sichere Nutzung zu beschreiben. Sie ist den Mitarbeitern als verbindliche Arbeitsanweisung bekannt zu machen und auch externen Nutzern der Anwendung verpflichtend vorzuschreiben.

Die Richtlinie sollte aus der Anwendung einfach erreichbar sein, z. B. durch einen Link aus dem Hilfe-Menü.

In der Richtlinie ist klar darzustellen:

- Wer ist zur Nutzung berechtigt.
- Welche Sicherheitsmaßnahmen sind einzuhalten.
- Nutzung der Anwendung ist nur nach erfolgreicher Authentifizierung gestattet. Die Nutzung von Sharing-Links mit oder ohne Passwort ist zu regeln.
- Welche Daten dürfen verteilt werden.
- Wer sind berechtige Empfänger der Daten.
- Wer ist bei Kenntnis über eine gewollte oder ungewollte Freigabe von Daten an Unberechtigte zu informieren.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in den folgenden Maßnahmen des IT-Grundschutzes:

- M 2.455 Festlegung einer Sicherheitsrichtlinie für Groupware

4.1.3 Planung von App-Nutzungen

Die Funktionalität von ownCloud kann durch Apps stark erweitert werden. In der Planung der Anwendung sind klare Regeln aufzustellen, welche Apps ownCloud benötigt, um das gewünschte Maß an Sicherheit und Funktionalität zu erreichen.

Auch an die Apps selbst sind Anforderungen zu stellen:

- Nur benötigte Apps dürfen installiert sein.
- Die Zahl der Apps ist möglichst klein zu halten.
- Apps des ownCloud Herstellers sind zu bevorzugen.
- Falls Apps von anderen Programmierern gewünscht sind, ist notwendig:
  - Sie sind vor dem Einsatz auf Sicherheitsprobleme zu überprüfen.
  - Benachrichtigungen bei neuen Versionen sind notwendige Voraussetzung für den Einsatz.
- Selbst entwickelte Apps sind nach Regeln für die sichere Softwareentwicklung zu erstellen und vor ihrem Einsatz auf Sicherheitsprobleme zu überprüfen.

4.1.4 Berechtigungen zum Teilen von Daten

Nur Administratoren haben das Recht, Berechtigungen zu setzen oder zu entfernen. Die Berechtigungen für das Teilen von Daten sind möglichst gering zu halten. Alle Berechtigungen sind in einem Betriebshandbuch zu dokumentieren, ownCloud selbst hat dafür keine Möglichkeit. Die betriebliche Notwendigkeit der Berechtigungen ist durch einen in der Organisation befindlichen Ansprechpartner zu begründen. In einem fest gelegten Zyklus von z.B. 2 Jahren sind die Berechtigungen zu überprüfen und nicht mehr benötigte zu deaktivieren.

Administratoren können folgende Einstellungen vorgeben:

- Anwender können Daten teilen, auch beschränkt auf vorgegeben Gruppen
- Anwender dürfen Daten öffentlich teilen
- Anwender müssen geteilte Daten mit Gültigkeitsdatum und/oder Passwortschutz einrichten
- Beschränken des Weiterverteilens
- Anwender dürfen Dritten, den Upload von Daten gestatten
- Anwender dürfen Mail-Benachrichtigungen über freigegebene Daten senden.

Das IT-Sicherheitsmanagement genehmigt Berechtigungen zum Teilen von Daten zu Organisationsfremden nach Antrag durch den Bedarfsträger und überprüft diese mindestens einmal im Jahr.

4.1.5 Schulung der Mitarbeiter und Nutzer

Bevor ein Mitarbeiter oder Organisationsfremder die Anwendung nutzen darf, ist er auf die Funktionen, Risiken und Regeln der Anwendung zu schulen. Die Inhalte der Schulung sind für die Nutzer zugänglich zu machen, so dass er jederzeit nachschlagen kann. Dies kann z.B. über die Hilfeseiten der Anwendung geschehen.

In der Schulung ist zu vermitteln:

- Bedienung der Anwendung
- Zweck der Anwendung und ihr Einsatz für die Organisation

- Inhalte der Richtlinie zu sicheren Nutzung
- Erkennen des Schutzbedarfs von Daten, um die Regeln der Richtlinie richtig anzuwenden.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in den folgenden Maßnahmen des IT-Grundschutzes:

- M 3.45 Planung von Schulungsinhalten zur Informationssicherheit

4.1.6 Architektur und Sicherheitsgateway

Die Architektur ist der geplanten Nutzung angemessen zu planen und umzusetzen. Es sind die Anforderungen der Verfügbarkeit, des Datendurchsatzes und der Sicherheit der zu verarbeiteten Daten festzulegen und zu beachten.

Sofern der Schutzbedarf der Daten bezüglich Verfügbarkeit höher als normal ist, ist eine redundante Architektur zu nutzen, in der die Lagerung und Verarbeitung der Daten auf mindestens zwei IT-Systemen parallel erfolgt. Die Aufstellung dieser beiden Stränge sollte auf mehrere Brandschutzzonen oder Gebäude verteilt sein.

Wenn die Anwendung auch aus Netzwerken außerhalb der Kontrolle der Organisation erreichbar ist, steht der Webserver in einem separaten Netzsegment und Sicherheitsgateways überwachen und beschränken die Verbindungen zu externen und internen Netzen. Bei größeren Umgebungen oder einem Schutzbedarf höher als normal, sollten der Webserver, die Datenbank und die Speichersysteme in jeweils eigenen Netzsegmenten innerhalb des Sicherheitsgateways stehen.

Die gemeinsame Nutzung von Datenbanken und Speichersystemen durch ownCloud und anderen Anwendungen ist vom Schutzbedarf der verarbeiteten Daten abhängig und die Architektur diesem angemessen zu planen.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in den folgenden Maßnahmen des IT-Grundschutzes:

- M 5.169 Systemarchitektur einer Webanwendung
- M 2.73 Auswahl geeigneter Grundstrukturen für Sicherheitsgateways

4.1.7 Rollen- und Rechte-Management

Nutzer im ownCloud erhalten die für sie geltenden Rechte über eine Zuordnung zu Gruppen. Die Zuordnung erfolgt entweder automatisch über einen Verzeichnisdienst oder manuell durch die Administration nach Antrag eines festzulegenden Personenkreises. So kann z. B. der Personalverantwortliche die Rollenzugehörigkeiten seiner Mitarbeiter bestimmen und diese bei der Administration in Auftrag geben.

Die Administration plant nach den Anforderungen der die Anwendung nutzenden Abteilungen die notwendigen Rollen und pflegt diese im ownCloud ein. Es ist darauf zu achten, dass jede Rolle nur die notwendigen Rechte beinhalten, aber auch nicht zu viele unterschiedliche Rollen definiert sind. Hier ist durch die Administration in Abstimmung mit dem IT-Sicherheitsmanagement abzuwägen und ein Mittelweg zu finden, zu dokumentieren und umzusetzen.

Definierte Rollen enthalten die Berechtigungen zum Freigeben von und Zugreifen auf Daten und sind wie diese regelmäßig auf ihre betriebliche Notwendigkeit hin zu überprüfen.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in den folgenden Maßnahmen des IT-Grundschutzes:

- M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen
- M 2.7 Vergabe von Zugangsberechtigungen

4.1.8 Authentifizierung Lokal

ownCloud kann die Nutzer über mehrere Wege authentifizieren. Nur in kleinen Umgebungen mit wenigen Nutzern ist die lokale Authentifizierung gegen die in der Anwendung enthaltene Benutzerverwaltung zu empfehlen.

Auch bei Benutzern, die auf der Anwendung selbst eingetragen sind, gelten die Regeln für die Vergabe von Rollen und Rechten.

Es sind per App starke Passwörter gemäß der bestehenden Passwortrichtlinie zu erzwingen.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in der folgenden Maßnahme des IT-Grundschutz:

- M 4.392 Authentisierung bei Webanwendungen

4.1.9 Authentifizierung mit Verzeichnisdienst

ownCloud kann diverse Verzeichnisdienste zur Authentifizierung der Nutzer einsetzen. Das Üblichste ist hierbei das Lightweight Directory Access Protocol (LDAP). Nutzer, die über einen Verzeichnisdienst authentifiziert werden, werden von ownCloud bei erstmaliger Anmeldung angelegt. Nutzer die im Verzeichnisdienst gelöscht oder deaktiviert sind, werden allerdings nicht automatisch aus dem ownCloud entfernt. Hier ist in regelmäßigen Abständen ein Abgleich durchzuführen, um die verwaisten lokalen ownCloud Nutzer zu deaktivieren.

Sofern LDAP im Einsatz ist, kann ownCloud diese Bereinigung über den Parameter „ldapUserCleanupInterval“ in der config.php automatisiert deaktivierte und gelöschte Benutzer identifizieren, deaktivieren und eine Liste der Accounts anzeigen. Die Administration kann dann entscheiden, ob sie diese Accounts löschen möchte. Zu beachten ist dabei, dass ownCloud dabei auch die Verzeichnisse löscht, die diesen Benutzern gehören.

Es ist darauf zu achten, dass ein technischer Benutzer im ownCloud hinterlegt ist, der ausreichende Berechtigungen zum Durchsuchen des LDAP besitzt.

Die Verbindung zwischen ownCloud und dem LDAP-Server sind zu verschlüsseln und das Zertifikat des Servers bei den Verbindungen zu überprüfen.

Um die Zahl der notwendigen Verbindungen zu reduzieren und so die Last auf dem LDAP zu verringern, sind erfolgreiche Anmeldungen für eine gewisse Zeit zu speichern. Die Länge der Zeit ist hierbei von der Organisation zu entscheiden. In der Regel ist dieser Zeitraum eine Stunde.

Die Berechtigung zur Nutzung von ownCloud ist über ein Merkmal im LDAP zu definieren. Dies kann per member-of-overlay auf dem LDAP Server oder als Filter im ownCloud geschehen.

Die Zugehörigkeit zu Gruppen im ownCloud ist über Gruppen im LDAP zu regeln. Hierfür sind entweder eigene Merkmale im LDAP einzurichten oder die bereits vorhandenen Gruppen sind im ownCloud zu nutzen.

ownCloud kann mehrere unterschiedliche Verzeichnisse einbinden. Dabei besteht keine Möglichkeit sicher zu stellen, dass die Accounts eindeutig sind. So kann eine Benutzer-ID in mehreren Verzeichnissen vorhanden sein und würde dann von ownCloud auf einen lokalen Benutzer zusammengeführt. Da so die Zuordnung der Handlungen zu einer Person nicht mehr gewährleistet ist, ist dieses Vorgehen nicht empfehlenswert.

Bei einem Schutzbedarf bezüglich Verfügbarkeit von höher als normal sind mehrere LDAP-Server einzusetzen, die entweder als Cluster redundant oder als mehrere einzelne LDAP-Server im ownCloud konfiguriert sind.

Neben LDAP kann ownCloud auch gegen IMAP, SMB und FTP authentifizieren. Da diese Dienste nur Authentifizierung ohne weitergehende Merkmale (Gruppen, Rechte, Rollen, etc.) der Accounts bieten und zusätzlich auch keine verschlüsselte Übertragung, wird von der Nutzung abgeraten.

4.1.10 Authentifizierung mit Federated-ID

ownCloud ist ein Mittel, um Daten auch über die Grenzen der eigenen Organisation hinaus zu verteilen. Dies bringt allerdings das Problem mit sich, dass es auch die organisationsfremden Personen authentifizieren muss. Eine Möglichkeit ist, die Personen als lokale Benutzer im Sharing-Dienst selbst anzulegen. Dies führt schnell zu veralteten Nutzerlisten, bei denen Benutzer noch im ownCloud aktiviert sind, die eigentlich nicht mehr berechtigt sind, da sie die eigene oder die Partner-Organisation verlassen haben. Siehe dazu die Gefährdung „Unberechtigte IT-Nutzung“.

Um die Nutzer aus mehreren Organisationen zuverlässig zu authentifizieren und sicher zu stellen, dass nur Personen mit einer gültigen Anmeldung auf die Anwendung zugreifen können, empfiehlt sich der Einsatz eines Federated-ID-Services. Hierbei werden die Verzeichnisdienste der anderen Organisationen genutzt und somit sind nur Personen anmeldeberechtigt, die auch zum Zeitpunkt des Anmeldevorgangs eine gültige Nutzerkennung in ihrer Organisation haben.

ownCloud setzt hierfür auf den im Apache Webserver als Modul erhältlichen Dienst Shibboleth und sofern SAML 2.0 unterstützt wird auch weitere IDPs. Der Nutzer meldet sich bei einem Shibboleth-Server seiner Organisation mit seinem dortigen Benutzeraccount an und erhält ein SAML Token. Dieses präsentiert der Browser des Nutzers dem Webserver, der bei vorhandener Vertrauensstellung den Nutzer akzeptiert und die Benutzer-ID dem ownCloud mitteilt. Der Benutzer ist damit am ownCloud angemeldet und sofern dies die erste Anmeldung ist, wird der lokale Account angelegt, so wie dies auch bei LDAP erfolgt. Wie auch dort, liegen allerdings auch bei federated ID keine Informationen vor, welche Nutzer entfernt oder deaktiviert sind. Daher ist es notwendig, in regelmäßigen Abständen ungenutzte Accounts zu entfernen.

Die Details der Konfiguration eines ID-Servers mit Shibboleth ist komplex und wird daher in diesem Dokument nicht behandelt[4].

Es ist allerdings darauf zu achten, dass die Vertrauensstellungen nur die betrieblich notwendigen Herausgeber von Tokens umfassen und dies nach Implementierung auch getestet wird.

Die erlaubten Benutzer der externen Organisation sind von dieser in ihrem ID-Server zu definieren, hier ist eine vertragliche Regelung über die Einhaltung der Anforderungen an die Sicherheit der Anwendung notwendig.

4.1.11 Einsatz von Verschlüsselung

Innerhalb von ownCloud wird Verschlüsselung an mehreren Stellen für die Absicherung der Kommunikation genutzt. Der Webserver darf nur per TLS ab Version 1.1 zugänglich sein, da sonst die Benutzernamen und Passwörter im Klartext übertragen werden würden. Aufgrund bekannter Schwachstellen bei SSL v2, v3 und TLS v1.0 ist von der Benutzung von dieser Protokolle dringend abzuraten. Dies gilt auch für die Anbindung an Verzeichnisdienste. Empfehlungen zum Einsatz von TLS sind in der jeweils aktuellen Fassung der Technischen Richtlinie TR-02102-2 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile) zu finden.

Eine Besonderheit von ownCloud ist die Verschlüsselung von Dateien durch den Server. Dabei agiert der ownCloud als Verschlüsselungsgateway. Der Nutzer erhält so unverschlüsselte Dateien, die aber auf den

4 Dokumentation ist zu finden unter: https://wiki.shibboleth.net/confluence/

Speichermedien verschlüsselt gelagert sind. Da die Verschlüsselung auf dem Server erfolgt, ist auch die Übertragung zum Speichermedium gesichert.

Zu beachten ist hierbei, dass nur die Inhalte der Dateien, aber weder ihr Name, noch der Name der Verzeichnisse verschlüsselt sind. Bereits diese Namen können einem Unbefugten Rückschlüsse auf den Inhalt erlauben, die nicht erwünscht sind und somit als Bruch der Vertraulichkeit gelten.

ownCloud verschlüsselt die Dateien dabei mit 256 Bit AES und einem 4096 Bit RSA Schlüssel pro Benutzer, der auf dem Server gespeichert ist.

Die Organisation ist gehalten, eine Regelung für die Verschlüsselung der Daten auf Datenträgern die über ownCloud angebunden sind zu definieren, zu dokumentieren und zu implementieren. Grundsätzlich gilt die Empfehlung, dass Daten auf Speichersystemen außerhalb der Verantwortung der eigenen Organisation zu verschlüsseln sind.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in der folgenden Maßnahme des IT-Grundschutz:

- M 5.66 Verwendung von TLS/SSL

4.1.12 Sichere Konfiguration

ownCloud ist eine in PHP geschriebene Anwendung, die einen Webserver zur Ausführung benötigt. Dies kann ein IIS (bis einschließlich Version 8.0) oder Apache (geplant ab Version 8.1) sein. Da der Betrieb mit Apache weit verbreitet ist, wird hier auf die sichere Konfiguration von Apache für ownCloud eingegangen. Die sichere Konfiguration von Apache ist ein weites Feld, das dieses Papier nicht vollständig darstellen kann. Für den sicheren Betrieb eines ownCloud mit Apache sind die folgenden Punkte mindestens zu beachten. Der Hersteller stellt auch einen Hardening-Guide[5] und eine Übersicht über allgemeine Absicherung der Betriebsumgebung[6] bereit.

Das Datenverzeichnis des ownCloud sollte nicht innerhalb des Webroot liegen, damit eine fehlerhafte Konfiguration des Apache nicht zur vollständigen Preisgabe der Daten an einen Unberechtigten Benutzer führen kann.

Auch ist auf die Sicherheit des PHP zu achten, Details sind im Sicherheitsdokument zu finden[7]. Das Suhosin Plugin[8] sollte installiert sein, da es die Absicherung stark verbessert.

Weitere Empfehlenswerte Module für den Apache sind mod_security, mod_evasive.

Um die von JavaScript und den Cookies genutzt Same-Origin Policy zu nutzen, empfiehlt es sich, den ownCloud Server in einer eigenen Domäne zu betreiben und nicht als Subdomain. Also besser owncloud.intern als owncloud.webapps.intern.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich im folgenden Baustein des IT-Grundschutz:

- B 5.4 Webserver

4.1.13 Anbindung externer Speicher

ownCloud erlaubt die Anbindung externer Speicher, wie z. B. Dropbox, Google Drive und Amazon S3. Der Einsatz ist in Abhängigkeit vom Schutzbedarf der verarbeiteten Daten zu regeln und mit dem IT-Sicherheitsmanagement abzustimmen.

5 https://doc.owncloud.org/server/8.1/admin_manual/configuration_server/hardening.html
6 https://owncloud.com/wp-content/uploads/2014/10/WP-Optimizing-ownCloud-Security-EN.pdf
7 https://php.net/manual/en/security.php
8 PHP Plugin Suhosin http://www.suhosin.org/

Wenn das ownCloud an externe Speicher angebunden ist, ist es damit automatisch auch mit Netzen verbunden, die nicht in der Verantwortung der Organisation stehen. Somit ist die Einbettung in eine Architektur mit Sicherheitsgateway notwendig.

Nur die Administration sollte die Rechte im ownCloud haben, externe Speicher einzubinden und nutzt hierfür einen technischen Benutzeraccount des Anbieters. Dieser Account benötigt ein sehr komplexes Passwort, das regelmäßig gewechselt wird.

Die Auslastung der externen Speicher ist zu beachten und eine Überwachung zu implementieren.

Wenn der Schutzbedarf der Daten eine verschlüsselte Speicherung auf dem externen Speicher erfordert, so ist die Serverseitige Verschlüsselung zu aktivieren.

4.1.14 Anbindung an Sharepoint

Sharepoint bietet die Option, auf Dateien über Listen zuzugreifen. Diese Listen kann ownCloud als externen Speicher einbinden und präsentiert sie dann den Benutzern wie ein Verzeichnis. Es nutzt für den Zugriff auf Sharepoint den Benutzernamen und Passwort des im ownCloud angemeldeten Nutzers oder einen globalen Account. Die Methode zur Authentifizierung ist in der Konfiguration pro Verzeichnis einzustellen.

Bei der Planung ist zu beachten, dass bei Nutzern die per ID-Server authentifiziert sind, kein Passwort vorliegt und diese daher nur die mit dem globalen Account angebundenen Verzeichnisse nutzen können.

Bei der Nutzung des globalen Accounts ist zu beachten, dass Sharepoint die hinterlegten Rechte auf die Daten nur gegen diesen Account prüfen kann. Bei Verzeichnissen wo detaillierte Rechte auf Daten anhand der Benutzerkennungen vergeben sind, sind daher die Anmeldedaten des Nutzers einzusetzen.

Diese Abhängigkeiten haben Auswirkungen auf die Planung der Benutzerverwaltung und Authentifizierung. So müssen alle Nutzer, die Sharepoint nutzen sollen, auch im vom Sharepoint genutzten Active Directory hinterlegt sein. Zumindest dann, wenn der globaler Account wegen der Rechtevergabe nicht zum Einsatz kommen darf.

4.1.15 Home Directories

Wenn ownCloud für die Authentifizierung LDAP gegen ein Active Directory nutzt, kann die Administration den Nutzern ihr Home-Directory im ownCloud bereit stellen.

Die Organisation ist gehalten zu entscheiden, ob die Home Directories genutzt werden und entsprechend zu implementieren.

4.1.16 Virenscanner

ownCloud bietet von Hause aus den OpenSource Virenscanner ClamAV zur Absicherung gegen die Übertragung von Malware über den Sharing-Dienst an. Da die Erkennungsraten dieses Werkzeuges nicht mit den etablierten, kommerziellen Produkten mithalten kann, ist bei Datenaustausch mit Organisationsfremden über den Sharing-Dienst dringend zu empfehlen, einen kommerziellen Virenscanner zu betreiben. Seit Version 7 ist dies möglich und ownCloud kann über die Antivirus App weitere Produkte einbinden. Es startet den Virenscanner über einen Kommandozeilenbefehl und übergibt die fragliche Datei als Pfad im lokalen Dateisystem.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in der folgenden Maßnahme des IT-Grundschutz:

- M 4.3 Einsatz von Viren-Schutzprogrammen

4.1.17 Anlegen von Verzeichnissen

Benutzer und Administratoren können in ownCloud Verzeichnisse anlegen. Wenn ein Benutzer gelöscht wird, löscht ownCloud auch die diesem Nutzer gehörenden Verzeichnisse und damit die enthaltenden Daten. Um dieses unerwünschte Verhalten zu vermeiden ist es notwendig, dass die Administration alle Verzeichnisse zentral anlegt. Dafür ist ein eigener Benutzeraccount zu verwenden, der keiner Person zugeordnet ist, um versehentliche Datenlöschungen zu vermeiden

4.1.18 Sicherheitsregeln File Firewall

Neben den Zugriffsrechten, der Anlage von Verzeichnissen und der Anbindung von externen Speichern bietet ownCloud noch eine weitere Methoden die Weitergabe von Dateien zu limitieren.

ownCloud beherrscht die regelbasierte Überprüfung von Freigaben und der Übertragung von Dateien. Wie eine Firewall legt es an jede Übertragung einen Satz Regeln an, die darüber entscheiden, ob es diese durchgeführt. Die Konfiguration erfolgt in der zentralen Konfigurationsdatei als Name-Wert paar im JSON Format und gilt für alle Verzeichnisse. Je nach Schutzbedarf der Daten und der Anbindung von externen Benutzern ist der Einsatz dieser Funktion zu erwägen, zu dokumentieren und zu planen.

Dieses Beispiel schränkt die Übertragung anhand der IP-Nummer ein:

```
{
"type": "condition",
"check": "cidr",
"cidr": "117.22.0.0/15",
"negate": true
}
```

Ab Version 8.0 gibt es für diesen Vorgang eine grafische Oberfläche. ownCloud filtert auf diese Merkmale:

- IP-Nummer
- Dateiname inklusive Pfad
- Subnetz
- Art des Zugriffs (Upload / Download)
- Benutzer / Benutzergruppe
- Zeit
- Größe

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in der folgenden Maßnahme des IT-Grundschutzes

- M 2.71 Festlegung einer Policy für ein Sicherheitsgateway

4.1.19 Server-zu-Server Sharing

Wie jedes Verzeichnis sollte die Verknüpfung mit anderen ownCloud Servern nur durch die Administration erfolgen dürfen.

Bei der Freigabe von Verzeichnissen an andere ownCloud Instanzen ist sicher zu stellen, dass die Notwendigkeit besteht dies zu tun und mit dem Schutzbedarf der Daten in diesem Verzeichnis vereinbar ist. In den meisten Fällen ist ein Passwort für die Freigabe einzurichten, es sollten nur in Ausnahmefällen Daten ohne Passwort freigegeben werden. Daher ist zu empfehlen, dass den Benutzern nicht das Recht eingeräumt wird, Freigaben ohne Passwort einzurichten, sofern die Benutzer dies überhaupt dürfen.

Die Lebensdauer der Freigabe und die Berechtigung zum Upload in dieses Verzeichnis ist nach betrieblicher Anforderung festzulegen und zu dokumentieren. Besonders ist zu beachten, dass keine Sharing-Dienste unterschiedlicher Sicherheitsstufen so miteinander verbunden sind, dass der Benutzer nicht erkennen kann, ob er die Daten auf diesem Verzeichnis speichern darf.

Die Sicherheitskonzepte verbundener Sharing-Dienste sind miteinander anzugleichen, um Lücken in der Sicherheit der Daten zu verhindern.

Die Administration sollte solche Freigaben in regelmäßigen Abständen auf den Fortbestand der Notwendigkeit der Freigabe kontrollieren und das Passwort wechseln, um sicher zu stellen, dass nur Berechtigte auf die Freigabe zugreifen dürfen.

Freigaben sind, sofern sie über öffentliche Netze die Daten transportieren, verschlüsselt auszuführen und die Gültigkeit der Zertifikate zu kontrollieren, um die Daten vor Einsichtnahme und gefälschten Sharing-Diensten zu schützen.

4.1.20 Protokollierung und Monitoring

Die Überwachung auf Verfügbarkeit und ausreichende Ressourcen des ownCloud Servers ist durch den Betreiber der Anwendung zu gewährleisten. Dies kann durch übliche Monitoring Werkzeuge, wie z. B. das frei verfügbare Nagios erfolgen.

Neben den Protokollen des Webservers sind auch die Protokolle des ownCloud per Syslog entweder lokal zu speichern oder an einen zentralen Protokoll-Server zu übertragen. Es ist empfehlenswert die eingehenden Protokolldaten automatisiert auf Hinweise zu Sicherheitsvorfällen zu untersuchen. Hierbei können verbreitete Analysetools wie Splunk hilfreich sein.

Da auch die Handlungen der Benutzer in den Protokollen mitgeschrieben sind, ist auf die Einhaltung der Bestimmungen des Datenschutzes zu achten und die Personalvertretung in die Entscheidungen einzubeziehen.

Nähere Beschreibungen – insbesondere für die Einbindung in ein Informationssicherheitsmanagementsystem – finden sich in den folgenden Maßnahmen des IT-Grundschutz:

- M 2.500 Protokollierung von IT-Systemen
- M 2.110 Datenschutzaspekte bei der Protokollierung

4.1.21 Anbindung an Berechtigungsmanagement

ownCloud ermöglicht es, über eine API die Provisionierung von Benutzern in der lokalen Benutzerverwaltung zu automatisieren. Werkzeuge zur Mitarbeiterverwaltung können so direkt auf die Benutzerlisten und Gruppen im ownCloud zugreifen und Einstellungen vornehmen. Es wird so sichergestellt, dass eine Änderung bei den Mitarbeitern auch sofort auf dem ownCloud ankommt. Dies kann ein Zugang, ein Abgang oder auch eine veränderte Gruppenzugehörigkeit sein.

Sollte der Sharing-Dienst keinen Verzeichnisdienst wie LDAP oder einen anderen Authentifizierungsdienst wie z.B. Shibboleth nutzen, ist zu empfehlen, die Verwaltung der lokalen Benutzer über diese API zu steuern.

4.2 Maßnahmen abhängig vom Betriebsmodell

4.2.1 Eigenbetrieb

In diesem Betriebsmodell ist die Organisation vollständig für die Sicherheit der Anwendung, der dort verarbeiteten Daten und der die Anwendung unterstützenden IT-Systeme verantwortlich.

Um die Sicherheit für alle Aspekte zu gewährleisten, muss ein Informationssicherheitsmanagementsystem in der Institution aufgebaut werden und ownCloud innerhalb dieses Systems behandelt werden. Ein solches ISMS ist der IT-Grundschutz. Im Rahmen eines Informationssicherheitsmanagementsystems wie z. B. IT-Grundschutz kann ownCloud modelliert werden und es sollten die Maßnahmen der identifizierten Bausteine in einer dem Schutzbedarf angemessenen Art und Weise umgesetzt werden.

4.2.2 Fremdbetrieb

Auch wenn der Betrieb in fremde Hände ausgelagert wird, verbleibt die Verantwortung für den sicheren Betrieb beim Inhaber der Inhalte, also des Auftraggebers. Nur die Umsetzung ist in die Verantwortung des Auftragnehmers gelegt. Daher ist es wichtig die aus dem Schutzbedarf entwickelten Sicherheitsziele und spezifischen Anforderungen mit dem Dienstleister vertraglich zu regeln.
Besonders ist darauf zu achten dass:

- Prozesse für die nahtlose Integration in das Benutzermanagement existieren,
- eine Berechtigungsvergabe für Verzeichnisse klar geregelt ist und
- die Anbindung von internen und externen Speichern unmissverständlich vorgeben ist.

Um die Sicherheit auch beim Fremdbetrieb zu gewährleisten, können die Maßnahmen des IT-Grundschutz Bausteins „B 1.11 Outsourcing“ herangezogen werden.

4.2.3 Hosting

Wie auch beim Fremdbetrieb ist auch beim Hosting der Anwendung darauf zu achten, dass die Verantwortung für den sicheren Betrieb beim Inhaber der Inhalte, also des Auftraggebers verbleibt. Nur die Umsetzung ist in die Verantwortung des Auftragnehmers gelegt. Daher ist es wichtig, die aus dem Schutzbedarf entwickelten Sicherheitsziele und spezifischen Anforderungen mit dem Dienstleister vertraglich zu regeln.

Um die Sicherheit auch beim Hosting zu gewährleisten, können die Maßnahmen des IT-Grundschutz Bausteins „B 1.11 Outsourcing“ herangezogen werden. Sofern die beim Anbieter betriebene Umgebung über ein VPN an die internen Netze der Organisation angebunden wird, sollten die Maßnahmen des IT-Grundschutz-Katalog Bausteins „B 4.4 VPN“ herangezogen werden.
Auch die Empfehlungen des „Eckpunktpapiers Cloud“ sind ein guter Anhaltspunkt.

4.2.4 Betrieb in der Cloud

Beim Software as a Service (SaaS) ist der Auftraggeber nur noch der Nutzer einer vollständig fremdbetriebenen Umgebung, die auch in den Räumen und Netzwerken des Auftragnehmers aufgestellt ist. Wie auch beim Hosting muss der Auftraggeber bei der Vertragsgestaltung mit einem Cloud-Anbieter weiterhin seinen Pflichten als Inhaber der Daten Rechnung tragen. Zu Fragen der Architektur, Sicherheit und technischen Umsetzung ist der Auftraggeber in der Pflicht die Anforderungen zu formulieren, wie dies im Abschnitt „Fremdbetrieb“ bereits beschrieben ist.

Zumeist gibt es allerdings wenig Gestaltungsspielraum, da die Angebote stark standardisiert sind. Hier ist es wichtig, einen Anbieter zu identifizieren, der die Anforderungen erfüllt und dies auch in seinen Verträgen

zusichert. Ein guter Hinweis sind dabei Zertifizierungen nach ISO 27001 (vorzugsweise auf der Basis von IT-Grundschutz) und – bei erhöhter Verfügbarkeitsanforderungen – ISO 22301. Ferner bieten die goldenen Regeln der Cloud-Bausteine des IT-Grundschutz eine gute Grundlage für einen Fragenkatalog an einen Anbieter.

5 Fazit

ownCloud bietet mit wenig Aufwand einen schnellen Start hin zum selbst betriebenen Sharing-Dienst. Es hilft dabei Grenzen zwischen Organisationen oder Geräten zu überwinden. Daten von einem Arbeitsplatz auf den anderen zu kopieren, geht per Fileserver sehr einfach. Zwischen Organisationen allerdings schon schwerer und wenn es darum geht, Dateien vom Arbeitsplatz auf ein Mobilgerät zu übertragen, kann ein Sharing Dienst eine große Hilfe sein.

Vor dem Einsatz sind die Möglichkeiten und die Limitationen genau abzuwägen. So kann ein ownCloud gut als Vermittler zwischen den Welten dienen und auch externe Personen in die Arbeitsprozesse einbinden, aber der Umfang der Funktionen ist im Vergleich zu anderen kommerziellen Produkten eingeschränkt. Das muss nicht unbedingt ein Nachteil sein, da manche Produkte durch ihre große Anzahl an Funktionen auch komplex in der Inbetriebnahme und Administration sind.

Auch zu betrachten sind die Cloud basierten Angebote, bei denen zwar der Betrieb und die Hoheit über die Daten komplett aus der Hand gegeben werden, aber die dafür auch die Aufwände für den Betrieb sehr reduzieren. Diese Überlegung ist auch für die Wahl des richtigen Betriebsmodells ausschlaggebend.

Ob ein Einsatz möglich ist, hängt immer vom Schutzbedarf der Daten ab. Jede Organisation sollte sich genau überlegen, wer welche Daten wann und wohin transportieren darf und welche Technik, welches Werkzeug dem Schutzbedarf und den betrieblichen Anforderungen am besten gerecht wird.

Unabhängig vom Betriebsmodell und auch vom Produkt ist die Verwaltung der Benutzer über die Grenzen der eigenen Organisation hinweg eine der Herausforderungen beim Betrieb eines Sharing-Dienstes. Hier ist genau zu planen und in der Umsetzung auf die Details der Vertrauensstellungen zu achten. Zu schnell öffnet sich durch den Sharing-Dienst ein Fenster in das eigene Netzwerk, durch das auch unerwünschte Gäste auf die Daten zugreifen können.