Optimale Sicherheit für Ihre ownCloud-Umgebung

Tipps und Tricks zur Verbesserung der Sicherheit

Eine aktuelle Studie des Marktforschungsunternehmens Harris Interactive hat ergeben, dass 38 % der Befragten bei der Arbeit Filesharing-Lösungen nutzen, die nicht von der IT-Abteilung genehmigt wurden. Das Unternehmen wird somit angreifbar und die Sicherheit der Daten erheblich beeinträchtigt. Zusätzlich verschärft wird das Risiko durch private elektronische Endgeräte die von über 80% der Angestellten bei der Arbeit genutzt werden.[1] Um diese Sicherheitslücken zu schließen, benötigen Unternehmen eine Filesharing-Lösung, die höchsten Sicherheitsanforderungen genügt, von der IT überwacht werden kann und sich einfach bedienen lässt.

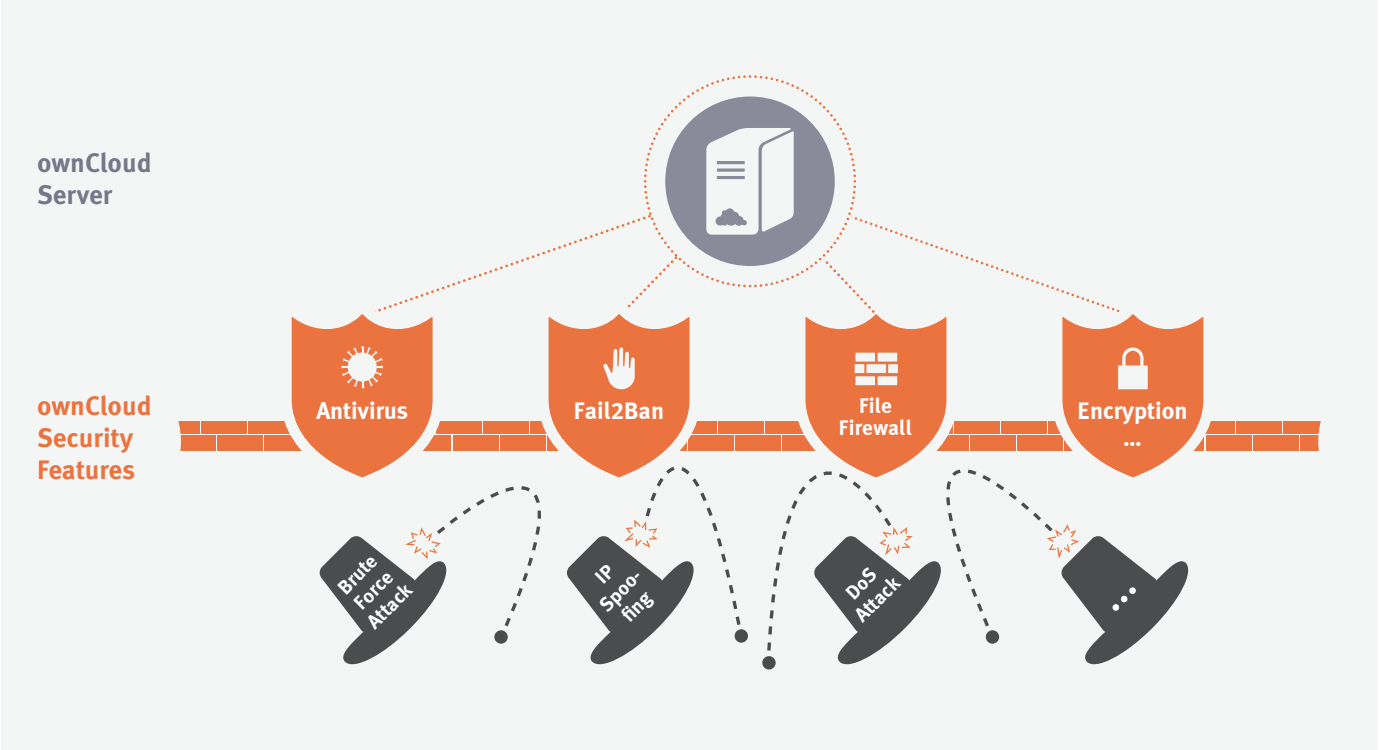

Abbildung 1: Die Sicherheitsfunktionen von ownCloud sorgen für einen zuverlässigen Schutz der auf dem ownCloud-Server gespeicherten Daten.

ownCloud sorgt für mehr Sicherheit beim Austauschen und Synchronisieren von Daten, Sie behalten jederzeit die volle Kontrolle über Ihre Dateien. Alle sensiblen Daten bleiben in Ihrem Unternehmen und gleichzeitig kann Ihre IT-Abteilung den Zugriff auf diese genau steuern. ownCloud bietet diese Sicherheit und wird den Erwartungen Ihrer Benutzer im Hinblick auf eine einfache Bedienung und eine hohe Produktivität gerecht.

Die Sicherheitsfunktionen von ownCloud

Im Gegensatz zu den für Endverbraucher konzipierten Cloud-Services bietet der ownCloud-Server der IT-Abteilung die Möglichkeit, sämtliche Elemente von ownCloud – vom Dateispeicher über das User Provisioning bis hin zur Datenverarbeitung – in der eigenen Umgebung zu verwalten und auf diese Weise optimal zu schützen. Der Server stellt ein sicheres Webportal zur Verfügung, über das der Administrator das gesamte System kontrollieren, Funktionen aktivieren und deaktivieren, Richtlinien festlegen und Benutzer verwalten kann.

[1] http://www.mobileauthenticationtoday.com/byod-swot-and-statistics/

Beim Austausch von Dateien kommt es entscheidend darauf an, dass die Sicherheit der Dateien gewahrt bleibt. Und genau deshalb sind Sicherheitsfunktionen integraler Bestandteil von ownCloud. Für die Integration von sekundären Speichergeräten verwenden wir ausschlieslich dokumentierte APIs bei denen Ihre bestehenden Hardware- und Governance-Richtlinien eingehalten werden. ownCloud kann zudem in die in Ihrem Unternehmen verwendeten Authentifizierungsdienste eingebunden werden, speichert jedoch selbst keine Anmeldedaten. Um mögliche Sicherheitslücken vollständig auszuschließen, schützt ownCloud Dateien im ownCloud-Speicher und während der Übertragung zusätzlich durch eine Verschlüsselung.

https://owncloud.com/de/end-to-end-encryption/

Sichern Sie Ihre Daten im eigenen Unternehmen
ownCloud wird im Rechenzentrum Ihres Unternehmens oder im Rechenzentrum eines Anbieters Ihrer Wahl auf physischen, virtuellen oder Private-Cloud-Servern betrieben.

Geben Sie der IT die volle Kontrolle
Ihre IT-Abteilung übernimmt die Kontrolle und Verwaltung von ownCloud. Administratoren verfügen mit ownCloud über eine Kontroll- und Verwaltungsinstanz, mit der sie Sicherheitsrichtlinien bis auf die Ebene der einzelnen Nutzer definieren, Benutzer, Gruppen und Quotas verwalten, Log-Dateien zur Netzwerkaktivität und die Integrität des Systems überwachen sowie die Nutzung des Systems protokollieren können.

Schützen Sie Ihre Investitionen
ownCloud kann nahtlos in die vorhandenen Benutzerverzeichnisse, Governance-Workflows, Sicherheitssyteme und Überwachungstools integriert werden und unterstützt viele gängige Speichertechnologien.

Automatisieren Sie die Authentifizierung
Integrierte Assistenzprogramme ermöglichen die Anbindung von ownCloud an Active Directory oder LDAP und die Authentifizierung mithilfe von SAML. Über das Web-Frontend, die mobilen Apps und die Desktop-Clients von ownCloud wird außerdem das auf SAML basierende Authentifizierungsverfahren Shibboleth unterstützt. Wenn Sie Ihre Benutzer mit diesen Diensten verwalten, verwendet ownCloud automatisch das dazugehörige Authentifizierungsverfahren.

Definieren Sie Zugriffsbeschränkungen auf mehreren Ebenen
Mithilfe von Zugriffsrechten auf Benutzer- oder Dateiebene kann genau festgelegt werden, wann und wo Dateien ausgetauscht werden dürfen. Der Zugriff auf Dateien kann auf mehreren Ebenen durch Passwortschutz und die Einrichtung eines Ablaufdatums gesteuert werden. Die File Firewall bietet Administratoren außerdem die Möglichkeit, den Zugriff auf die ownCloud-Server zu kontrollieren, indem sie Zugriffsrechte für bestimmte Verbindungen, Zeiträume, Standorte und andere Kriterien vergeben. Zusätzlich können Administratoren das Sharing, falls notwendig, mit CRUDS überschreiben.

Schützen Sie sich erfolgreich vor Viren und Malware
ownCloud untersucht Dateien beim erstmaligen Hochladen auf den Server mit ClamAV auf Viren und Malware und verhindert so die automatische Verbreitung infizierter Dateien. Mit nur wenigen Einstellungen kann die Software auch so konfiguriert werden, dass Dateien beim Hochladen auf den Server durch externe Virenscanner überprüft werden.

Umfassende Auditing-Möglichkeiten
Sie können mit ownCloud nicht nur die Zugriffsrechte der einzelnen Benutzer steuern, sondern darüber hinaus auch einen vollständigen Audit Trail anlegen. So können Sie jederzeit genau nachvollziehen, wie, wann und wo auf Ihre Daten zugegriffen wird. Mithilfe von zwei separaten Apps können Administratoren die Aktivitäten auf Account-Ebene protokollieren, beispielsweise anhand der Logins bei ownCloud oder der Verwendung der Dateien auf dem Server. Damit verfügen Administratoren über alle wichtigen Informationen, die sie für das Compliance Reporting und das Auditing der ownCloud-Nutzung benötigen. Zugleich sind Sie mit diesen Tools in der Lage, sämtliche Aktivitäten beim Filesharing aktiv zu überwachen. Von zusätzlicher Sicherheit proftieren Sie, indem Sie die Logs so konfigurieren, dass sie automatisch an einen Enterprise Log Manager wie SPLUNK weitergeleitet werden.

Best Practices für die Konfiguration von ownCloud

Zwar enthält ownCloud bereits zahlreiche integrierte Sicherheitsfunktionen, doch sollte eine ownCloud-Umgebung immer auch an die Sicherheitsstandards und -richtlinien des Unternehmens angepasst werden. So vermeiden Sie, dass Ihre Daten Risiken ausgesetzt werden. Mit den folgenden Best Practices können Sie die Sicherheit Ihrer ownCloud-Umgebung weiter optimieren:

Vermeiden Sie Schwachstellen in Ihrer Firewall: Wenn Sie in Ihrer Firewall Ports für die Datenübertragung freigeben, sollten Sie die erforderlichen Sicherheitsvorkehrungen treffen und die freigegebenen Ports sorgfältig überwachen. Beschränken Sie die Portfreigaben auf die Ports, die Sie wirklich für die Übertragung benötigen, damit Ihre Firewall möglichst wenig Angriffsfläche bietet. Sorgen Sie für eine lückenlose Überwachung aller offenen Ports, da ein offener und nicht überwachter Port eine große Gefahr darstellt. In den meisten ownCloud-Umgebungen muss lediglich ein Port freigegeben werden – Port 443 für den TLS/SSL-Datenverkehr.

Schützen Sie gemeinsam genutzten Arbeitsspeicher: Über gemeinsam genutzten Arbeitsspeicher können sich Angreifer Zugriff auf Dienste verschaffen, die gerade ausgeführt werden. Schützen Sie Ihre Umgebung deshalb mit fstab vor möglichen Angriffen. Die genauen Einstellungen für fstab hängen vom verwendeten Betriebssys-

tem ab. Um beispielsweise bei einem System mit Ubuntu 12.04 LTS den gemeinsam genutzten Arbeitsspeicher zu schützen, können Sie den folgenden Eintrag unter /etc/fstab erstellen:

```
tmpfs /dev/shm tmpfs
defaults,noexec,nosuid 0 0
```

Secure Shell (SSH): Der beste Schutz für SSH ist ein Login mit öffentlichem und privatem Schlüssel. Wenn Ihr Login-Verfahren jedoch die Eingabe von Benutzernamen und Passwort voraussetzt, deaktivieren Sie einfach den Root-Benutzer und ändern Sie den Port, um die Angriffsmöglichkeiten zu verringern.

Schützen Sie Ihre Server durch Beschränkung des Zugriffs auf die Admin-Gruppe: Auch wenn diese Sicherheitsmaßnahme eine Selbstverständlichkeit sein sollte, wird sie doch häufig vergessen. Wenn Sie ownCloud-Webserver außerhalb Ihrer Firewall betreiben, sollten Sie den Zugriff auf diese Server auf die Admin-Gruppe beschränken, um möglichst wenig Angriffsfläche zu bieten.

Verbessern Sie die Netzwerksicherheit durch sysctl-Einstellungen: sysctl ist ein Interface, über das in BSD- und Linux-Betriebssystemen Parameter untersucht und dynamisch geändert werden können. Durch Ändern der Konfigurationsdatei sysctl.conf können folgende Einstellungen vorgenommen werden:

1. Netzwerkkonfiguration um den IPv4 Traffic einzuschränken
2. Netzwerkkonfiguration um den IPv6 Traffic einzuschränken
3. Aktivieren des Schutzes mit Exec Shield
4. Schutz vor SYN-Flood-Angriffen
5. Überprüfung der IP-Adresse des Quellsystems
6. Vermeiden von Spoofing-Angriffen auf die IP-Adresse des Servers
7. Protokollieren von verdächtigen Paketen wie z. B. gefälschten Paketen, Source-Routed-Paketen und Redirect-Paketen

Deaktivieren Sie die offene DNS-Rekursion und unterdrücken Sie die Versionsnummer – Bind9 DNS: Auch wenn es keine gängige Praxis ist, werden DNS-Server und Webserver gelegentlich auf demselben System gehostet. In einem solchen Fall sollten Sie potenziellen Angreifern möglichst wenig Informationen über Ihre Umgebung zugänglich machen. Hierzu müssen Sie lediglich in den Optionen der Datei named.conf einstellen, dass diese Informationen NICHT angezeigt werden.

Unterbinden Sie IP-Spoofing: Diese Schutzmaßnahme verhindert, dass Ihr Netzwerk Ziel eines Spoofing-Angriffs wird, bei dem bei der Kommunikation über das Netzwerk die IP-Adresse des Absenders gefälscht wird. Spoofing wird vor allem bei DoS-Angriffen verwendet. Aktivieren Sie mit folgendem Befehl die reverse Pfadfilterung (rp_filter):

```
echo 1 >  /proc/sys/net/
ipv4/conf/all/rp_filter
```

Dadurch wird die Standardschnittstelle erstellt. Das Spoofing wird unterbunden, indem sichergestellt wird, dass die Quelladresse des Pakets über die Schnittstelle erreichbar ist, über die es empfangen wurde. Alternativ kann auch eingestellt werden, dass die Quelladresse über jede verfügbare Instanz erreicht werden kann. Pakete, deren IP-Quelladresse nicht zurückverfolgt werden kann, werden verworfen.

Sichern Sie PHP ab: Zwar wurden einige Sicherheitseinstellungen bereits von Ihrem Softwareanbieter vorkonfiguriert, doch können Sie bei der Einrichtung Ihrer Server zusätzliche Schutzmaßnahmen ergreifen.

- Lesen Sie zu diesem Thema auch die Beschreibungen und Tipps im PHP-Handbuch unter http://php.net/manual/en/security.php.
- Durch Einbindung der PHP-Sicherheitserweiterung Suhosin in Ihre Installation können Sie PHP wie unter http://www.suhosin.org/stories/feature-list.html beschrieben absichern.
- Verhindern Sie, dass Apache Informationen zur Version Ihres Webservers preisgibt, indem Sie das Banner mit den entsprechenden Versionen abschalten. Dadurch verfügen potenzielle Angreifer nicht über Detailinformationen zur Softwareversion Ihres Servers, mit denen sie nach bekannten Schwachstellen suchen können.
- Konfigurieren Sie in der Datei https.conf die Parameter „ServerTokens“ und „ServerSignature“ mit den folgenden Einstellungen:
  ServerTokens Prod
  ServerSignature Off

Installieren Sie ModSecurity: ModSecurity besteht aus einer Firewall für Webanwendungen, die auf Apache, IIS und Nginx installiert werden kann und Administratoren zusätzliche Kontrollmöglichkeiten bietet. Das Apache-Modul stellt Optionen für das Protokollieren zufallsbasierter Angriffe, Funktionen für die Echtzeitüberwachung des Datenverkehrs mit Warnfunktionen und vieles mehr bereit. ModSecurity ist speziell darauf ausgerichtet, die Angriffsfläche Ihrer Webanwendungen zu verringern. Hierzu verwendet das Modul Heuristikfilter zur Erkennung verdächtiger Zugriffsmuster oder erlaubt ausschließlich Zugriffe auf tatsächlich angeforderte Ressourcen (Whitelist) und gibt nur angefragte Werte zurück.

Installieren Sie Mod_evasive: Das Modul Mod_evasive schützt Apache vor HTTP-DoS- oder HTTP-DDoS-Angriffen. Sie können das Tool so konfigurieren, dass Zugriffsbeschränkungen gültiger IP-Adressen vermieden werden und zugleich eine Blacklist verdächtiger IP-Adressen erstellt wird, über die automatische Angriffe auf Ihre ownCloud-Instanz ausgeführt werden können. Mit dem Modul lassen sich beispielsweise Regeln für die Erkennung folgender Angriffsmuster implementieren:

- Eine bestimmte Seite wird mehr als x Mal pro Sekunde angefordert.
- Eine bestimmte IP-Adresse wird mehr als x Mal pro Sekunde gleichzeitig angefordert.
- Es wird versucht, über gesperrte IP-Adressen (Blacklist) zuzugreifen.

Überwachen Sie Log-Dateien mit Tools wie Fail2Ban: Nutzen Sie Tools zur Überwachung von Log-Dateien. Mit dem Tool Fail2Ban werden beispielsweise die Apache-Logs auf verdächtige Aktivitäten untersucht. Die Firewall wird dynamisch aktualisiert, sodass verdächtige IP-Adressen blockiert werden. Sie können das Tool Ihren Anforderungen entsprechend konfigurieren und dadurch das Risiko von Brute-Force-Angriffen auf Ihr System verringern.

Intrusion Detection: Mithilfe von Tools wie PSAD können Sie iptables-Logs auf verdächtige Aktivitäten wie Port-Scans und anderen fragwürdigen Datenverkehr untersuchen. Sie profitieren damit von präemptiven Untersuchungen Ihres Systems und können Angriffe proaktiv abwehren.

Aktivieren Sie SELinux oder AppArmor: Diese Technologien verbessern die Sicherheit Ihres Systems, indem bei der Kontrolle des Datei- und Netzwerkzugriffs der Sicherheitskontext berücksichtigt wird. Damit lassen sich die Risiken unbefugter Systemzugriffe minimieren. SELinux und AppArmor werden häufig einfach deaktiviert, da sie bei falscher Konfiguration die Installation und Nutzung von Anwendungen und Datenbanken erschweren.

Überwachen Sie Log-Dateien: Für die kontinuierliche Überwachung der Systemintegrität empfiehlt es sich, wichtige Log-Dateien laufend zu überwachen. Hierzu gehören neben der Log-Datei von ownCloud auch Log-Dateien des Systems, der Webserver und von Apache. Die zentrale Überwachung dieser Log-Dateien mit einem Tool wie SPLUNK ermöglicht das einfache Erstellen von Dashboards, über die Sie Echtzeitinformationen zur Sicherheit Ihres Systems anzeigen können.

Im Rahmen des ownCloud Deploy Service Package bietet Ihnen ein technischer Berater von ownCloud Hilfestellung bei der Einrichtung dieser Überwachungsfunktionen, mit denen Sie Ihr System zuverlässig schützen können.

TLS/SSL: Auch wenn die TLS/SSL-Verschlüsselung inzwischen Standard sein sollte, raten wir dringend dazu, die gesamte Kommunikation mithilfe von TLS/SSL-Protokollen zu verschlüsseln.

Virenschutz: Für einen optimalen Virenschutz empfiehlt ownCloud die Aktivierung von ClamAV. Diese Virenschutzanwendung ist in der ownCloud Enterprise Edition enthalten. Mit ClamAV werden infizierte Dateien entfernt und können somit Ihre Nutzer nicht erreichen.

Im Rahmen des ownCloud Deploy Service Package bieten Ihnen Berater von ownCloud Hilfestellung bei der Konfiguration Ihrer Umgebung. Über unser Kontaktformular unter owncloud.com/de/kontakt können Sie einen Beratungstermin mit uns vereinbaren.

ownCloud GmbH
Rathsbergstr. 17
90411 Nürnberg
Germany

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

owncloud.com

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