Absicherung Ihrer Daten in der Cloud mit den umfassendsten Sicherheits- und Verschlüsselungsmechanismen

Die Vorteile von MozyPro

Einfach

Nahtlose Verwaltung, Synchronisation und mobiler Zugriff auf Backups für Multianwender- und Serverumgebungen von einer einzelnen, webbasierten Konsole aus.

Sicher

Ihre Daten befinden sich in erstklassigen Datenzentren. Verschiedene Verschlüsselungsschlüssel bieten maximale Sicherheit. EMC – ein Unternehmen, das Bestand hat.

Kostengünstig

Sparen Sie Kosten ein; die Anschaffung von Hardware ist nicht erforderlich und die Betriebskosten sind auf ein Minimum reduziert.

Kontakt zu MozyPro

emeasales@mozy.com
0800 1808227
www.mozy.de/pro

Mehr als nur Datenbackups

Cloudbasierte Backuplösungen erfreuen sich wachsender Beliebtheit, da sie effektive Datensicherheit und Geschäftskontinuität mit hoher Zuverlässigkeit und Konsistenz leisten können, während IT-Kosten sowie Wartungs- und Supportaufwand deutlich reduziert werden. Bevor Unternehmen die Vorteile eines Cloudbackupservice nutzen können, müssen jedoch die vom Serviceprovider eingesetzten Sicherheits- und Verschlüsselungsmethoden genauer betrachtet werden. Als einer der führenden Provider von Cloudbackupservices der Branche nimmt Mozy den Schutz Ihrer Daten in der Cloud sehr ernst und trifft dazu umfassendste Sicherheits- und Datenschutzvorkehrungen.

Sicherheit

Mozy verschlüsselt Ihre Daten schon auf Ihrem Computer, während des Übertragungsprozesses selbst und in unseren Rechenzentren (Data-at-Rest-Verschlüsselung). In den EMC Rechenzentren kommen modernste physische und technische Sicherheitsmaßnahmen zum Einsatz, die mit den Datenschutzgrundsätzen des Safe-Harbor-Abkommens der Europäischen Union im Einklang stehen. Darüber hinaus hat Mozy erfolgreich ein SSAE 16-Audit vom Typ 2 (SOC 1) bestanden und wurde gemäß ISO 27001 zertifiziert. Die unabhängigen Nachweise bestätigen, dass die Prozesse und Verfahren von Mozy die strengsten Kontrollziele der Branche erfüllen oder übertreffen. Durch die freiwillige Durchführung eines SSAE 16-Audits und die Erlangung einer Zertifizierung nach ISO 27001 demonstriert Mozy den Stellenwert, den der Schutz von Kundeninformationen und die Bekämpfung laufender Bedrohungen für digitale Informationen genießen. Viele verbreitete cloudbasierte Backupservices können solche hohen Sicherheitsstandards nicht erfüllen. So werden Ihre Daten bei einigen Services nicht vollständig sicher verschlüsselt oder bleiben sogar völlig unverschlüsselt. Weiter unten in diesem Dokument werden die umfassenden Maßnahmen und Optionen ausführlich beschrieben, mit denen Mozy die optimale Sicherung und Verschlüsselung Ihrer Daten ermöglicht.

Verschlüsselungsstandards und -optionen bei Mozy

Noch bevor Ihre Backupdaten Ihren Computer verlassen, werden sie von Mozy einer AES- oder Blowfish-Verschlüsselung unterzogen. Blowfish ist ein Public-Domain-Algorithmus, der 1993 von dem bekannten Kryptografen Bruce Schneier entwickelt wurde. Blowfish wurde als schneller Algorithmus für allgemeine Zwecke entwickelt und nutzt eine sichere symmetrische Blockchiffre mit variabler Schlüssellänge. Mozy nutzt beim Einsatz des Blowfish-Algorithmus die maximale Schlüssellänge von 448 Bit.

Der Branchenstandard AES ist ein 256-Bit-Verschlüsselungsalgorithmus, der auch von US-Behörden als allgemeiner Standard zur Verschlüsselung geheimer und streng geheimer Informationen verwendet wird. AES wird auch von der NSA (National Security Agency) als Standardalgorithmus eingesetzt und ist inzwischen einer der am häufigsten unterstützten und genutzten Verschlüsselungsalgorithmen überhaupt. Außerdem erfüllt der AES-Algorithmus die Sicherheitsanforderungen für kryptografische Module gemäß FIPS 140-2 (Federal Information Processing Standard, US-Bundesstandard für Informationsverarbeitung). Da durch die Nutzung der AES-Verschlüsselung sämtliche behördlichen Datenschutzstandards erfüllt werden, können auch Regierungsbehörden und entsprechend reglementierte Abteilungen für den Schutz ihrer Daten auf die AES-Verschlüsselungsoptionen von Mozy vertrauen.

Obwohl AES als allgemein sicherer oder stärker als Blowfish bekannt ist, gelten beide Algorithmen als sehr sicher. Auch erzielt AES zwar schnelle Verschlüsselungsraten, bleibt dabei jedoch hinter Blowfish zurück.

Der Blowfish-Algorithmus gilt zwar als sicher, allerdings gibt es keine öffentlich zugängliche Kryptoanalyse dieses Algorithmus. Das bedeutet jedoch nicht, dass der Algorithmus unsicher ist, sondern nur, dass eventuell vorhandene Schwächen noch nicht bekannt sind. Außerdem ist dies ein Hinweis darauf, dass andere, bekanntere Algorithmen möglicherweise langfristig weiter verbreitet sein werden. Andererseits wurde AES mehrfach sehr ausführlich geprüft. Erstmals wurde im Rahmen der Einführung als erweiterter Verschlüsselungsstandard ein fünf Jahre dauernder Prüfprozess durchgeführt. Seit dem Jahr 2000 wurden zahlreiche weitere öffentlich zugängliche Kryptoanalysen von AES durchgeführt. In der Folge hat sich der Algorithmus schließlich als einer der sichersten verfügbaren Algorithmen überhaupt durchgesetzt.

Verschlüsselungstypen

Ob Sie mit dem MozyPro-Service die AES- oder Blowfish-Verschlüsselung nutzen, wird durch Ihre Entscheidung für eine der folgenden drei Mozy-Verschlüsselungsoptionen bestimmt, die jeweils bestimmte Vorteile bieten:

- **Mozy-Standardchiffrierschlüssel:** Mozy weist Ihren Anwendern einen Chiffrierschlüssel zu. Dieser Schlüssel wird nahtlos von Mozy gespeichert und gemanagt. Dieser Schlüssel nutzt die Blowfish-Verschlüsselung.
- **Persönlicher Chiffrierschlüssel:** Der Anwender gibt eine Passphrase ein, um den Chiffrierschlüssel zu erstellen. Jeder Anwender erstellt einen eindeutigen persönlichen Chiffrierschlüssel. Dieser Schlüssel nutzt die AES-Verschlüsselung.
- **Unternehmenschiffrierschlüssel:** Der Administrator gibt eine Passphrase ein, um den Chiffrierschlüssel zu erstellen. Sie können einen Schlüssel für alle Anwender im Unternehmen oder einen eindeutigen Schlüssel für jede Anwendergruppe erstellen. Der Unternehmensschlüssel wird manchmal als C-Schlüssel bezeichnet. Dieser Schlüssel nutzt die AES-Verschlüsselung.

Der Typ des verwendeten Chiffrierschlüssels wird während der Installation der Mozy-Software festgelegt. Dieser Verschlüsselungstyp wird dauerhaft für die in der EMC Cloud gespeicherten Dateien verwendet. MozyPro-Kunden können den Verschlüsselungstyp konfigurieren, indem sie ihren Anwendern über eine Clientkonfiguration den entsprechenden Chiffrierschlüsseltyp zuweisen. Der Verschlüsselungstyp kann nach der Installation der Software geändert werden. In diesem Fall werden alle Dateien erneut hochgeladen, damit die gespeicherten Dateien immer mit dem aktuell konfigurierten Chiffrierschlüssel verschlüsselt werden.

Unabhängig vom verwendeten Chiffrierschlüsseltyp werden alle Dateien im ersten Verarbeitungsschritt verschlüsselt, bevor sie an die EMC Cloud gesendet werden. Dadurch sind Ihre Dateien jederzeit sicher – bevor sie Ihren Computer verlassen, während der Übertragung und in der EMC Cloud (Data-at-Rest-Verschlüsselung). Wenn Sie persönliche Chiffrierschlüssel verwenden, kann Mozy den Schlüssel weder lesen noch weitergeben. Ihre Dateien können also in keinem Fall entschlüsselt werden, bevor Sie sie auf Ihrem Computer wiederherstellen.

Zusätzlich zur AES- oder Blowfish-Verschlüsselung verwendet Mozy zur Übertragung Ihrer Daten eine zertifizierte SSL-Verbindung mit beidseitiger Zertifikatbestätigung. Über diese Verbindung wird die gesamte Kommunikation zwischen Ihren Computern und dem MozyPro-Dienst abgewickelt. Diese Technologie wird auch von Banken zur Absicherung von Onlinetransaktionen eingesetzt. Darüber hinaus müssen sich alle Anwender bei Mozy mit einem registrierten Benutzernamen und Passwort authentifizieren.

Mozy-Standardchiffrierschlüssel

Der Standardchiffrierschlüssel nutzt den Blowfish-Algorithmus für die Verschlüsselung Ihrer Daten. Neben der hohen Sicherheit und Geschwindigkeit dieses Algorithmus besteht einer der Hauptvorteile der Verwendung des Standardchiffrierschlüssels darin, dass Mozy diesen Schlüssel für Sie verwaltet. Daher besteht für Sie kein Risiko, die Passphrase für diesen Schlüssel zu vergessen, wenn Sie Ihre Daten ver- oder entschlüsseln möchten. Mozy übernimmt diese Aufgaben automatisch für Sie und sorgt dafür, dass Ihre Daten schon vor der Übertragung während des Backupprozesses sicher verschlüsselt werden.

Darüber hinaus bieten die Mobilitäts- und Webfunktionen von Mozy integrierten Support für den Standardchiffrierschlüssel. Somit können Sie alle Backupdateien über Ihr mobiles Gerät oder einen Webbrowser nahtlos und sicher anzeigen, durchsuchen oder herunterladen. Der Standardschlüssel bietet für Ihre gesamten Backups eine sofortige und anwenderfreundliche Verschlüsselung. Obwohl der Standardschlüssel eine sichere und anwenderfreundliche Verschlüsselung bietet, bevorzugen einige Unternehmen das Management ihrer eigenen Passphrase für die Verschlüsselung, statt diesen Schlüssel gegenüber Mozy bekannt zu machen. Wie der Name nahelegt, wird der Standardchiffrierschlüssel standardmäßig verwendet, sofern Sie keine andere Verschlüsselungsoption wählen.

Persönlicher Chiffrierschlüssel

Ein persönlicher Chiffrierschlüssel ist eine von zwei Optionen, die Mozy Unternehmen oder Einzelpersonen anbietet, die AES-Verschlüsselung nutzen möchten. Persönliche Chiffrierschlüssel ermöglichen einzelnen Anwendern das Management ihrer eigenen Chiffrierschlüssel. Dazu legt jeder Anwender einen eigenen eindeutigen Chiffrierschlüssel für die Daten auf seinem Computer fest. Zusätzlich zur ohnehin schon stärkeren Sicherheit von AES wird die Sicherheit durch einen eindeutigen, nur dem Einzelanwender bekannten Schlüssel nochmals erhöht. Dieser Schlüssel wird nicht vom Mozy-Service verwaltet und ist Mozy nicht bekannt. Daher kann Mozy Ihre Dateien unter keinen Umständen entschlüsseln, wenn Sie die persönliche Verschlüsselung wählen – auch nicht, wenn dies per Gesetz gefordert würde.

Um ihren eindeutigen persönlichen Chiffrierschlüssel zu generieren, werden Anwender zur Eingabe einer Passphrase aufgefordert, die Buchstaben, Sonderzeichen oder Zahlen enthalten kann. Die Passphrase kann beliebig lang sein. Zur sicheren Aufbewahrung des Schlüssels nutzt die Mozy-Clientsoftware einen kryptografischen Hash der auf dem Computer des Anwenders gespeicherten Passphrase. Da der Mozy-Service persönliche Chiffrierschlüssel nicht speichert und nicht entschlüsseln kann, müssen Sie die entsprechende Passphrase eingeben, um Ihre gesicherten Dateien über die Web- und mobilen Funktionen von Mozy anzeigen, durchsuchen oder direkt herunterladen zu können.

Wenn Sie als Mozy-Administrator eine Wiederherstellung für Ihre Anwender durchführen oder die Dateien von Anwendern wiederherstellen möchten, die das Unternehmen verlassen haben, müssen Sie die persönlichen Chiffrierschlüssel der entsprechenden Anwender kennen oder Zugriff darauf haben.

Ebenso können Einzelanwender, die ihre Passphrase vergessen, ihre Daten auf einer Workstation weder entschlüsseln noch wiederherstellen. Zur Vorbeugung vergessener Passphrases bietet Mozy die Exportoption an. Über die Exportoption kann der Anwender die Passphrase für die Verschlüsselung als Textdatei auf einem Netzwerkshare oder USB-Wechsellaufwerk speichern. Sie kann zwar auch auf der Festplatte des lokalen Computers gespeichert werden; dies wird jedoch nicht empfohlen, da der Zugriff auf diese Datei bei einem Systemfehler des Computers nicht mehr möglich wäre. Wir empfehlen Unternehmen, für die Nutzung der Exportoption eine Sicherheits-Policy zur Bestimmung des Speicherorts dieser Passphrase-Dateien festzulegen.

Unternehmen, die die AES-Verschlüsselung nutzen, ihre Anwender aber keine eigenen Passphrases managen lassen möchten, bietet Mozy den Unternehmenschiffrierschlüssel als Option an.

Unternehmenschiffrierschlüssel

Mit dem Unternehmenschiffrierschlüssel (manchmal als C-Schlüssel bezeichnet) können Unternehmen bei der Verschlüsselung ihrer Daten von der Sicherheit des AES-Algorithmus profitieren und gleichzeitig das Passphrase-Management deutlich vereinfachen. Bei dieser Option legt eine Einzelperson die Passphrase für das gesamte Unternehmen fest. Diese Einzelperson kann beliebig bestimmt werden, z. B. eine Führungskraft im Bereich IT oder Sicherheit, ein Manager oder Administrator.

Über die Mozy-Administrationskonsole werden die Passphrase für den Unternehmensschlüssel und deren Speicherort festgelegt. Dieser kann z. B. ein Netzwerkshare, ein Webserver oder ein Paket für die Installation von Mozy auf Clientcomputern sein. Da Mozy auf unterschiedlichen Computern verwendet wird, greift jeder Computer auf diesen Speicherort zu, um Dateien mit dem Chiffrierschlüssel zu ver- und entschlüsseln.

Da die Passphrase für den Unternehmenschiffrierschlüssel häufig auf einem Netzwerkshare oder Webserver gespeichert wird, nutzt Mozy eine Shared-Secret-Funktion zur Verschlüsselung der Passphrase, um diesen Schlüssel vor unbefugtem Zugriff zu schützen. Bei der Installation von Mozy auf den Clientcomputern wird die Verschlüsselung dieser Passphrase automatisch auf jedem Client programmiert. Somit können alle Workstations, auf denen der Mozy-Backupclient ausgeführt wird, mit dieser Passphrase nahtlos Dateien ver- oder entschlüsseln.

Wie auch bei persönlichen Chiffrierschlüsseln kann Mozy Ihnen keine Hilfestellung bei der Entschlüsselung gesicherter Dateien leisten, da wir keinen Zugriff auf den Unternehmenschiffrierschlüssel haben. Unternehmenschiffrierschlüssel werden von allen Anwendern im Unternehmen oder innerhalb einer Anwendergruppe gemeinsam verwendet und können entweder auf den lokalen Computern oder auf einem Netzwerkserver gespeichert werden.

Erstklassige Rechenzentren

Die hochmodernen Rechenzentren von EMC sind gemäß SSAE 16 geprüft und nach ISO 27001 zertifiziert und verfügen über folgende Sicherheitsvorkehrungen:

- **Vor-Ort-Monitoring und -Sicherheit:** Alle Rechenzentren befinden sich innerhalb eines sicheren Perimeters und werden rund um die Uhr von Technologieexperten betreut, die auf die Einhaltung höchster Datensicherheitsstandards achten. Der Zutritt zu den Einrichtungen und Servern von Mozy ist ausschließlich nach sowohl kartenbasierter als auch biometrischer Sicherheitsauthentifizierung möglich.
- **Brandmelde- und Brandbekämpfungsanlagen:** Alle von EMC verwalteten Rechenzentren sind mit Gaslöschanlagen ausgestattet, mit denen Brände bekämpft werden können, ohne die Funktion der Server zu beeinträchtigen.
- **Redundante Stromversorgungen und Netzwerke:** Die Stromversorgung unserer Rechenzentren wird durch redundante Systeme realisiert und geschützt. Darüber hinaus werden alle Rechenzentren von mehreren Netzwerkprovidern betreut, sodass ein unterbrechungsfreier Betrieb auch bei einem Ausfall eines Netzwerkbetreibers möglich ist.
- **Temperaturkontrolle:** Alle Rechenzentren sind mit Kühlmechanismen ausgestattet, damit die Server jederzeit optimalen Betriebstemperaturen ausgesetzt sind.

Da Mozy zudem mehrere Rechenzentren an internationalen Standorten unterhält, können Daten lokal innerhalb wirtschaftlicher Communitys gespeichert werden. Dadurch können Daten etwa innerhalb der USA oder der EU aufbewahrt werden. So wird die Einhaltung lokaler Gesetze und Vorschriften zur Datenverarbeitung ermöglicht.

Datenschutz

Um den Datenschutz bei Ihren Daten zu wahren, nutzt Mozy eine Kombination aus technischen, administrativen und physischen Kontrollmechanismen, um personenbezogene Daten gemäß Branchenstandards zu schützen. Darüber hinaus hat Mozy eine eigene Datenschutzverpflichtung aufgestellt, gemäß der wir nach den folgenden Grundsätzen arbeiten:

- Ihre Informationen gehören Ihnen und nicht uns.
- Wir verkaufen niemals Ihre Informationen oder Informationen über Sie weiter.
- Wir durchsuchen niemals Ihre Informationen zu Profilierungs- oder Werbezwecken.
- Sie können Ihre Informationen jederzeit zurückfordern. Wir behalten keinerlei Rechte an Ihren Informationen, wenn Sie den Service nicht mehr nutzen.

Schützen Sie Ihre Daten und Ihr Unternehmen

Wenn Sie Informationen mit Mozy sichern, behalten Sie über die Authentifizierungs- und Verschlüsselungsmechanismen des Systems die Kontrolle über die Daten. Jede in der Mozy-Cloud gespeicherte Datei wird vor der Übertragung in unsere Infrastruktur verschlüsselt, sodass die Vertraulichkeit privater Informationen jederzeit gewahrt bleibt. Wir üben keinen Einfluss auf die internen Sicherheitsmaßnahmen aus, die unsere Kunden zur Einhaltung verschiedener Vorschriften durchführen. Mozy unternimmt zudem proaktive Schritte zum Schutz vor Angriffen, Gefahren oder unbefugtem Zugriff, um einer Gefährdung der Sicherheit, Vertraulichkeit oder Integrität Ihrer Daten vorzubeugen.

Die Aufgabe von Mozy ist die Absicherung Ihrer Daten und Ihres Unternehmens. Sie können sich auf unsere strengen Sicherheitsrichtlinien, Branchenstandard-Verschlüsselung und erstklassigen Rechenzentren verlassen, mit deren Hilfe Mozy die Verfügbarkeit, Sicherheit und Vertraulichkeit bietet, die für den optimalen Schutz Ihrer geschäftlichen Daten erforderlich sind.

Ein zuverlässiger Partner

Mozy sichert Daten für mehr als 100.000 Unternehmen und mehr als 6 Millionen Einzelpersonen und verwaltet Daten im Umfang von 90 Petabyte. Als Teil des führenden Speicheranbieters EMC, einem Fortune 200-Unternehmen, spielt Mozy eine zentrale Rolle bei der Verpflichtung von EMC für den Schutz Ihrer geschäftskritischen Daten. EMC bietet die technologische Infrastruktur und die Lösungen, mit denen Unternehmen wettbewerbsfähig bleiben und ihre Informationen optimal nutzen können. Aufgrund unserer Geschichte als eines der ersten Cloud-Computing-Unternehmen und unsere Partnerschaft mit EMC verfügt Mozy über die nötige Erfahrung, die Infrastruktur und die Finanzkraft, um die Sicherheit und Verfügbarkeit Ihrer Daten zu jedem Zeitpunkt zu ermöglichen. Mozy von EMC ist bei Fortune 500- wie bei kleinen Unternehmen gleichermaßen als zuverlässigster Partner für Cloudbackups renommiert.