mozyenterprise®

Schutz und Verschlüsselung von Online-Backups

Der Vorteil von MozyEnterprise

Einfach

Verwalten Sie Umgebungen mit vielen Anwendern, planen Sie automatische Backups und überwachen Sie die Integrität Ihrer Backups über eine praktische, webbasierte Admin-Konsole.

Sicher

Mozy ist SSAE 16 geprüft, ISO 27001 zertifiziert, benützt nur die strengsten Sicherheitsmaßnahmen, Verschlüsselungstechnologie auf militärischem Niveau und Weltklasse-Rechenzentren.

Kostengünstig

MozyEnterprise fügt sich nahtlos in die existierende IT-Architektur ein, ohne Datenbänder, DVDs oder Hardware zu benötigen und hält Ihre IT-Managementkosten auf ein Minimum.

Kontakt MozyEnterprise

emeacorporatesales@mozy.com
T 0800 1808227
www.mozy.de/enterprise

Laut IDC sind die Online-Backupdienste mittlerweile das größte und beliebteste Segment der modernen Cloud-basierten Speicherdienste (The Benefits of Cloud-Based Backup, IDC September 2011). Die Zunahme der Cloud-basierten Backups lässt sich darauf zurückführen, dass sie effektive Datensicherheit und Geschäftskontinuität bereitstellen und damit zu mehr Zuverlässigkeit und Konsistenz und gleichzeitig zu einer deutlichen Senkung der IT-Kosten und des Aufwands für die laufenden Wartungs- und Supportmaßnahmen führen. Allerdings müssen Unternehmen die Sicherheits- und Verschlüsselungsmethoden des Dienstanbieters genau überprüfen, bevor sie einen Online-Backupdienst nutzen. Als einer der branchenführenden Anbieter von Online-Backupdiensten nimmt Mozy den Schutz Ihrer Daten sehr ernst. Beim Schutz von Daten in der Cloud gilt unsere Aufmerksamkeit vor allem drei Problembereichen: Sicherheit, Datenschutz und Compliance.

Sicherheit

Mozy verschlüsselt die Daten, bevor sie Ihren Computer verlassen, bei der Übertragung und während sie sich in unseren Rechenzentren befinden. Die Rechenzentren erfüllen durch ihre modernen physischen und technischen Sicherheitsmaßnahmen die höchsten Anforderungen und sind (sofern relevant) an die „Safe Harbor"-Vereinbarung gebunden (European Union Safe Harbor Privacy Principles). Außerdem erfüllt Mozy den Audit-Standard SSAE-16 und ist ISO 27001-zertifiziert. Diese unabhängigen Überprüfungen belegen, dass die Prozesse und Verfahren von Mozy die strengsten Kontrollziele der Branche erfüllen oder übertreffen. Durch die freiwillige Durchführung des SSAE-16-Audits und den Erwerb der ISO 27001-Zertifizierung zeigt Mozy sein Engagement für die Sicherheit der Kundendaten und die Vorbereitung auf die zunehmenden Bedrohungen für digitale Informationen. Von den beliebten Cloud-basierten Backupdiensten sind viele nicht in der Lage, derart hohe Sicherheitsstandards zu implementieren. Bei einigen Diensten ist die Verschlüsselung der Daten nicht ausreichend sicher, bei anderen wird sie gänzlich vernachlässigt. Dieses White Paper beschreibt detailliert die umfassenden Maßnahmen und Optionen, mit denen Mozy sicherstellt, dass Ihre Daten nach dem neuesten Stand der Technik geschützt und verschlüsselt werden.

Verschlüsselungsoptionen und -standards von Mozy

Bevor die Backupdaten Ihren Computer verlassen, werden sie von Mozy mit AES oder Blowfish verschlüsselt. Blowfish ist ein Public-Domain-Algorithmus, der 1993 von dem bekannten Kryptographen Bruce Schneier entwickelt wurde. Dieser schnelle Allzweck-Algorithmus beruht auf einer sicheren symmetrischen Blockverschlüsselung mit variabler Länge. Wenn Mozy den Blowfish-Verschlüsselungsalgorithmus einsetzt, wird die maximale Schlüssellänge von 448 Bit verwendet.

AES ist ein militärtauglicher 256-Bit-Verschlüsselungsstandard, der von der US-amerikanischen Regierung für geheime und streng geheime Daten verwendet wird. Er wird auch von der National Security Agency eingesetzt und gehört mittlerweile zu den am besten unterstützten und am häufigsten verwendeten Verschlüsselungsalgorithmen. Zudem entspricht der AES-Algorithmus dem Federal Information Processing Standard (FIPS) 140-2 für Kryptografie. Ein Unternehmen, das die AES-Verschlüsselung einsetzt, erfüllt damit alle staatlichen Datenschutzstandards. Alle Regierungsbehörden und die ihnen unterstellten Verwaltungseinheiten können zum Schutz ihrer Daten die AES-Verschlüsselungsoptionen von Mozy verwenden.

Obwohl AES im Vergleich zu Blowfish annerkannter und sicherer angesehen wird, gelten beide Algorithmen als äußerst sicher. AES erreicht hohe Verschlüsselungsgeschwindigkeiten, wird in diesem Punkt jedoch von Blowfish noch übertroffen.

Obwohl Blowfish als sicher angesehen wird, fehlt eine öffentlich verfügbare Kryptoanalyse des Algorithmus. Dies bedeutet jedoch nicht, dass der Algorithmus selbst fehlerhaft ist, sondern dass Schwächen – sofern vorhanden – bisher nicht bekannt sind. Andere Algorithmen, denen mehr Aufmerksamkeit gewidmet wurde, können sich im gewerblichen Einsatz möglicherweise länger behaupten und werden auf breiterer Basis unterstützt. Im Gegensatz zu Blowfish wurde AES wiederholt strengen Prüfungen unterzogen. Die erste Prüfung dauerte 5 Jahre und war Teil der Einführung als Advanced Encryption Standard. Seit dem Jahr 2000 wurden zahlreiche weitere Kryptoanalysen zu AES veröffentlicht. Dies führte zu einer breiten Akzeptanz und machte AES zu einem der sichersten Verschlüsselungsalgorithmen auf dem Markt.

Ob der MozyEnterprise-Dienst Ihre Daten mit AES oder Blowfish verschlüsselt, hängt davon ab, welche der folgenden Mozy-Verschlüsselungsoptionen Sie verwenden:

- Standardschlüssel: Blowfish
- Persönliche Schlüssel: AES
- Enterprise privater Schlüssel: AES

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 MozyEnterprise-Dienst abgewickelt. Mit derselben Technologie wird im Bankwesen die Sicherheit von Online-Transaktionen gewährleistet. Alle Benutzer müssen sich bei Mozy mit einem registrierten Benutzernamen und einem Kennwort authentifizieren.

Standardmäßiger Verschlüsselungsschlüssel

Der standardmäßige Verschlüsselungsschlüssel (kurz: Standardschlüssel) verschlüsselt Ihre Daten mit dem Blowfish-Algorithmus. Einer der Hauptvorteile des Standardschlüssels besteht darin, dass er nicht nur mit einem äußerst sicheren und schnellen Verschlüsselungsalgorithmus verknüpft ist, sondern auch von Mozy für Sie verwaltet wird. Sie müssen sich keine Passphrase für diesen Schlüssel merken, wenn Sie Daten verschlüsseln oder entschlüsseln möchten. Mozy übernimmt dies automatisch für Sie und sorgt auf diese Weise dafür, dass Ihre Daten sicher verschlüsselt sind, bevor sie im Rahmen eines Backups übertragen werden.

In den Mobilitäts- und Webfunktionen von Mozy ist die Unterstützung des Standardschlüssels bereits integriert. Dadurch können Sie Backupdateien über ein Mobilgerät oder einen Webbrowser sicher und verzögerungsfrei anzeigen, durchsuchen und herunterladen. Der Standardschlüssel garantiert die konfigurationsfreie und benutzerfreundliche Verschlüsselung Ihrer gesamten Backups. Einige Unternehmen ziehen es dennoch vor, eine eigene Verschlüsselungs-Passphrase zu verwenden, anstatt den Schlüssel von Mozy verwalten zu lassen. Wie der Name bereits vermuten lässt, wird der Standardschlüssel standardmäßig verwendet, wenn Sie keine der anderen Verschlüsselungsoptionen wählen.

Persönlicher Verschlüsselungsschlüssel

„Persönliche Schlüssel“ ist eine der beiden Mozy-Optionen für Unternehmen und Einzelpersonen, welche die Vorteile der AES-Verschlüsselung nutzen möchten. Die Option erlaubt einzelnen Benutzern, ihre eigenen Verschlüsselungsschlüssel zu verwalten. Wenn diese Option verwendet wird, legt jeder Benutzer seinen eigenen eindeutigen Verschlüsselungsschlüssel für die Daten auf seinem Computer fest. So wird die hohe Sicherheit von AES noch durch einen eindeutigen Schlüssel verbessert, der nur dem betreffenden Benutzer bekannt ist. Der Mozy-Dienst hat keine Kenntnis von diesem Schlüssel und verwaltet ihn auch nicht. Wenn Sie einen persönlichen Verschlüsselungsschlüssel verwenden, kann Mozy also unter keinen Umständen – auch nicht auf dem Rechtsweg – veranlasst werden, Ihre Dateien zu entschlüsseln.

Beim Einrichten eines eindeutigen persönlichen Schlüssels wird der Benutzer aufgefordert, eine aus Buchstaben, Symbolen und Ziffern bestehende Passphrase einzugeben. Die Passphrase kann von beliebiger Länge sein. Damit der Schlüssel sicher ist, verwendet die Client-Software von Mozy einen kryptografischen Hash der auf dem Rechner des Benutzers gespeicherten Passphrase.

Da der Mozy-Dienst Ihren persönliche Verschlüsselungsschlüssel weder speichert noch ihn entschlüsseln kann, müssen Sie die richtige Passphrase eingeben, wenn Sie gesicherte Dateien mit den Mobilitäts- und Webfunktionen von Mozy anzeigen, durchsuchen oder direkt herunterladen möchten.

Wenn Sie Mozy-Administrator sind und eine Wiederherstellung im Auftrag eines Benutzers durchführen oder die Dateien eines Benutzers, der nicht mehr beim Unternehmen tätig ist, wiederherstellen möchten, müssen Sie den persönlichen Verschlüsselungsschlüssel dieses Benutzers kennen oder darauf Zugriff haben.

Ebenso können Benutzer, die ihre Passphrase vergessen haben, ihre Daten nicht mehr entschlüsseln oder auf einer Workstation wiederherstellen. Zum Schutz gegen vergessene Passphrasen dienen die Export von Mozy. Die Exportoption erlaubt dem Benutzer, die Verschlüsselungs-Passphrase als reine Textdatei auf einem Netzlaufwerk oder einem Wechseldatenträger (USB) zu speichern. Die Passphrase kann auch auf der Festplatte des lokalen Computers gespeichert werden. Dies wird jedoch nicht empfohlen, da in diesem Fall bei einem Systemfehler kein Zugriff auf die Datei möglich ist. Jedes Unternehmen, in dem die Exportoption eingesetzt wird, sollte in einer Sicherheitsrichtlinie festlegen, wo Passphrase-Dateien gespeichert werden dürfen.

Ein Unternehmen, das die Vorteile der AES-Verschlüsselung nutzen möchte, ohne Benutzer ihre eigenen Passphrasen verwalten zu lassen, kann die Option „Enterprise privater Schlüssel“ verwenden.

Unternehmens-Verschlüsselungsschlüssel (Enterprise privater Schlüssel)

Die Mozy-Option „Unternehmensschlüssel (Enterprise privater Schlüssel)“ erlaubt einem Unternehmen, bei der Verschlüsselung von Daten die Stärken des AES-Algorithmus zu nutzen und zugleich die Verwaltung der Passphrasen erheblich einfacher und sicherer zu gestalten. Mit der Option „Enterprise privater Schlüssel“ wird der Passphrasen-Schlüssel für das gesamte Unternehmen von einer einzigen Person eingerichtet. Diese Person kann ein beliebiger Mitarbeiter sein, z. B. der IT-Leiter, der Sicherheitschef, ein Manager oder ein Administrator. In der Mozy-Administratorkonsole legen Sie die Enterprise privater Schlüssel-Passphrase und ihren Speicherort fest (z. B. ein Netzlaufwerk, einen Webserver oder ein Paket, mit dem Mozy auf Client-Rechnern installiert wird). Wenn Mozy auf verschiedenen Rechnern eingesetzt wird, greift jeder der Rechner auf diesen Speicherort zu und verwendet den Verschlüsselungsschlüssel zum Verschlüsseln und Entschlüsseln von Dateien.

Da die Enterprise privater Schlüssel-Passphrase meist auf einem Netzlaufwerk oder einem Webserver gespeichert wird, verschlüsselt Mozy sie mithilfe einer Funktion namens „Freigegebenes Geheimnis“, die den Schlüssel gegen unbefugten Zugriff schützt. Wenn Sie Mozy auf den verschiedenen Client-Rechnern installieren, wird die verschlüsselte Passphrase automatisch auf jedem der Clients abgelegt. Dadurch können Workstations, auf denen der Mozy-Backupclient läuft, auf die Passphrase zugreifen und Dateien ohne Verzögerung verschlüsseln und entschlüsseln.

Wenn Sie die Option „Enterprise privater Schlüssel“ verwenden und eine Web-Wiederherstellung durchführen möchten, müssen Sie die Dateien, die wiederhergestellt werden sollen, mit dem Kryptodienstprogramm von Mozy entschlüsseln. Das Kryptodienstprogramm von Mozy fordert Sie auf, den Pfad der Enterprise privater Schlüssel-Datei, das freigegebene Geheimnis und die von der Web-Wiederherstellung heruntergeladenen Dateien anzugeben. Dann werden die Dateien entschlüsselt und auf Ihrem lokalen Rechner wiederhergestellt.

Da die Enterprise privater Schlüssel-Passphrase wie ein persönlicher Schlüssel von Ihnen selbst verwaltet und gespeichert wird, ist sie Mozy vollkommen unbekannt. Im Gegensatz zu anderen Providern von Online-Backups ist es bei Mozy nicht erforderlich, den Schlüssel zum Mozy-System hochzuladen oder dort zu hinterlegen. Dies hat zur Folge, dass Mozy nicht in der Lage ist, Ihre Dateien zu entschlüsseln, wenn Sie die Option „Enterprise privater Schlüssel“ verwenden. Da weder der Mozy-Dienst noch die meisten Benutzer in Ihrem Unternehmen Zugriff auf Ihre Enterprise privater Schlüssel-Passphrase haben, ist außerdem sichergestellt, dass die Unternehmensdaten vor unbefugtem Zugriff geschützt sind. Das gilt auch dann, wenn Mitarbeiter versuchen, Dateien auf einen Heimcomputer herunterzuladen.

mozyenterprise®

Datenschutz

Um die Vertraulichkeit Ihrer Daten zu gewährleisten und Ihre persönlichen Daten zu schützen, kombiniert Mozy technische, administrative und physische Kontrollen, die dem neuesten Stand der Technik entsprechen. Außerdem wurde bei Mozy eine eigene Datenschutzverpflichtung eingeführt, die auf den folgenden Geschäftsprinzipien beruht:

- Ihre Informationen gehören Ihnen, nicht uns.
- Wir werden niemals versuchen, Ihre Informationen zu verkaufen, und wir verkaufen keine Informationen über Sie.
- Wir filtern niemals Ihre Informationen, um ein Profil von Ihnen zu erstellen oder gezielt Werbung an Sie weiterzuleiten.
- Sie können Ihre Informationen jederzeit zurückfordern. Wir haben keine Rechte an Ihren Informationen, wenn Sie den Dienst kündigen.

Compliance

Für Mozy gehört die Compliance zu den wichtigsten Faktoren beim Datenschutz. Unsere Kunden treten oft mit der Frage an uns heran, ob unsere Backuplösungen mit den verschiedenen internationalen, US-amerikanischen und europäischen Standards konform sind, z. B. mit PCI DSS, SOX, HIPAA, GLBA, den Richtlinien 95/46/EG (Datenschutzrichtlinie) und 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) sowie der Safe-Harbor-Liste. Hinter diesen Standards steht das Prinzip, dass der Eigentümer stets die Kontrolle über vertrauliche Daten behalten soll und dass nur autorisierte Personen Zugriff auf diese Daten erhalten dürfen.

Wenn Sie bei Mozy Daten sichern, garantieren die vom System verwendeten Authentifizierungs- und Verschlüsselungsfunktionen, dass Sie die Kontrolle über Ihre Daten behalten. Jede in der Mozy-Infrastruktur gespeicherte Datei wird vor der Übertragung verschlüsselt. Ihre privaten und vertraulichen Daten bleiben privat und vertraulich, solange wir sie für Sie aufbewahren. Die internen Sicherheitskontrollen, mit denen unsere Kunden die Compliance mit verschiedenen Bestimmungen sicherstellen, bleiben bei Mozy in vollem Umfang wirksam. Mozy unternimmt vorbeugende Schritte zum Schutz gegen Angriffe, unautorisierten Zugriff und sonstige Gefahren, die die Sicherheit, Vertraulichkeit und Integrität Ihrer Daten bedrohen.

Schützen Sie Ihre Daten und Ihr Unternehmen

Mozy garantiert professionellen Schutz für Ihre Daten und damit für Ihr Unternehmen. Vertrauen Sie auf die strengen Sicherheitsrichtlinien, die militärtaugliche Verschlüsselung und die erstklassigen Rechenzentren von Mozy. Wir bieten Verfügbarkeit, Sicherheit, Vertraulichkeit und Compliance und sorgen für den optimalen Schutz Ihrer Unternehmensdaten. Von Fortune 500-Unternehmen bis hin zu Kleinunternehmen ist Mozy der führende Anbieter von Online-Backuplösungen. Als Tochtergesellschaft des Speichergiganten EMC verfügt Mozy über die nötige Erfahrung und Infrastruktur zum Schutz Ihrer wertvollen Daten.