iCloud: Überblick über Sicherheit und Datenschutz

http://support.apple.com/kb/HT4865

Bei Apple werden die Datensicherheit und der Schutz Ihrer persönlichen Informationen sehr ernst genommen. iCloud baut auf Sicherheitsverfahren gemäß Branchenstandard auf und es gelten strikte Richtlinien, um Ihre Daten zu schützen.

In diesem Artikel wird erläutert, wie iCloud Ihre persönlichen Informationen und Daten sicher schützt.

Zusätzliche Informationen finden Sie in der Apple Datenschutz-richtlinie, die auch für iCloud gilt.

Datensicherheit

iCloud schützt Ihre Daten, indem sie verschlüsselt über das Internet übertragen sowie in einem verschlüsselten Format auf dem Server abgelegt werden (Einzelheiten finden Sie in der folgenden Tabelle). Für die Authentifizierung werden sichere Tokens verwendet. Dies bedeutet, dass Ihre Daten sowohl bei der Übertragung an Ihre Geräte als auch bei der Speicherung in der Cloud vor unbefugtem Zugriff geschützt sind. iCloud arbeitet mindestens mit einer 128-Bit-AES-Verschlüsselung, der gleichen Sicherheitsstufe, die auch große Finanzinstitute anwenden. Verschlüsselungsschlüssel werden niemals an Dritte weitergegeben.

Sicherheit und iCloud-Funktionen

In der folgenden Tabelle ist zusammenfassend dargestellt, wie Ihre Daten bei der Verwendung der verschiedenen iCloud-Funktionen abgesichert werden:

Daten	Verschlüsselung		Hinweise
	Bei Übertragung	Auf dem Server	
Kalender	Ja	Ja	Mindestens mit 128-Bit AES verschlüsselt
Kontakte	Ja	Ja	
Lesezeichen	Ja	Ja	
Erinnerungen	Ja	Ja	
Fotos	Ja	Ja	
Dokumente in der Cloud	Ja	Ja	
Backup	Ja	Ja	
Mein iPhone suchen	Ja	Ja	
Freunde suchen	Ja	Ja	

iCloud-Schlüsselbund	Ja	Ja	Verwendet die 256-Bit-AES-Verschlüsselung zur Speicherung und Übertragung von Kennwörtern und Kreditkartendaten. Verwendet auch die asymmetrische Elliptische-Kurven-Kryptographie und den Key-Wrap-Algorithmus.
iCloud.com	Ja	Keine Angabe	Alle Sitzungen auf iCloud.com werden mit SSL verschlüsselt. Jegliche Daten, auf die über iCloud.com zugegriffen wird, werden wie in dieser Tabelle angegeben auf dem Server verschlüsselt.
Zugang zu meinem Mac	Ja	Keine Angabe	Bei der Verwendung von "Zugang zu meinem Mac" werden keine Daten in iCloud abgelegt. Von anderen Computern abgerufene Daten werden bei der Übertragung mit SSL verschlüsselt.
iTunes in der Cloud	Ja	Keine Angabe	Gekaufte und abgeglichene Musikdateien werden auf dem Server nicht verschlüsselt, da sie keine persönlichen Daten enthalten.
Mail und Notizen	Ja	Nein	Jeglicher Datenverkehr zwischen Ihren Geräten und iCloud Mail und Notizen wird mit SSL verschlüsselt. Gemäß der branchenüblichen Praxis werden die in iCloud auf IMAP-Mail-Servern gespeicherten Daten nicht verschlüsselt. Alle Apple-E-Mail-Clients unterstützen die optionale S/MIME-Verschlüsselung.

Verwendung sicherer Token zur Authentifizierung

Wenn Sie über integrierte Apple-Apps (zum Beispiel Mail, Kontakte und Kalender unter iOS oder OS X) auf iCloud-Dienste zugreifen, erfolgt eine Authentifizierung mithilfe eines sicheren Tokens. Bei der Verwendung sicherer Token müssen Sie Ihr iCloud-Kennwort nicht auf Geräten und Computern sichern. Selbst wenn Sie mithilfe eines Programms eines Drittanbieters auf Ihre iCloud-Daten zugreifen, werden Ihr Benutzername und Kennwort über eine verschlüsselte SSL-Verbindung übertragen.

Starke Kennwörter

Beim Erstellen einer Apple ID zur Verwendung mit iCloud müssen Sie ein Kennwort wählen, das mindestens 8 Zeichen umfasst und eine Ziffer, einen Großbuchstaben und einen Kleinbuchstaben enthält. Die Verwendung eines starken Kennworts ist die wichtigste Maßnahme zum Schutz Ihrer Daten. Hier erhalten Sie weitere Informationen zum Erstellen eines sicheren Kennworts.

Datenschutz

Ihre Privatsphäre wird in allen Bereichen des Unternehmens Apple respektiert. In unserer Datenschutzrichtlinie wird dargelegt, wie wir Ihre Daten erfassen, nutzen, offenlegen, übertragen und speichern.

Die iCloud-Funktionen wurden nicht nur unter Berücksichtigung der Apple Datenschutzrichtlinie, sondern auch mit dem Schutz Ihrer Privatsphäre als zentrales Anliegen konzipiert. z. B.:

Mein iPhone suchen

Damit Ihr Gerät geortet werden kann, müssen Sie in den iOS-Einstellungen die Funktion "Mein iPhone suchen", "Mein iPad suchen" bzw. "Meinen iPod touch suchen" einschalten.

Um Ihren Mac zu orten, müssen Sie in den Mac OS X-Systemeinstellungen die Funktion "Meinen Mac suchen" einschalten.

Ihr Gerät versendet nur dann Standortdaten, wenn Sie dessen Standort abfragen. Diese Daten werden zu keinem anderen Zeitpunkt übermittelt oder aufgezeichnet.

Die Informationen zum letzten bekannten Gerätestandort werden 24 Stunden lang in einem verschlüsselten Format auf den Apple-Servern gespeichert und anschließend unwiederbringlich gelöscht.

Daten im Modus "Verloren" werden auf dem Gerät gespeichert, das sich im Modus "Verloren" befindet, und können nur durch Ihre Anfrage abgerufen werden.

Nach 15 Minuten Inaktivität werden Sie automatisch von der App "Mein iPhone suchen" (auf dem Gerät bzw. im Internet) abgemeldet.

Mit der Funktion "Fernsperre" können Sie den Bildschirm eines Gerätes sperren, um zu verhindern, dass Dritte auf Ihre Daten zugreifen können.

Mit der Funktion "Fernlöschen" können Sie Ihre Daten sicher und unwiederbringlich von einem Gerät löschen.

Weitere Informationen zu "Mein iPhone suchen"

Freunde suchen

Um die Funktion "Freunde suchen" verwenden zu können, müssen Sie zunächst die optionale und kostenlose App "Meine Freunde suchen" im App Store laden.

Damit andere Ihren Standort angezeigt bekommen, müssen Sie diesen Personen zunächst die ausdrückliche Erlaubnis erteilen.

Ihr Gerät versendet nur dann Standortdaten, wenn ein Freund Ihren Standort abfragt. Diese Daten werden zu keinem anderen Zeitpunkt übermittelt oder aufgezeichnet.

Es gibt einen Schalter, mit dem Sie Ihren Standort jederzeit vor all Ihren Freunden verbergen können.

Die Informationen zum letzten bekannten Standort werden nur 2 Stunden lang in einem verschlüsselten Format auf den Apple-Servern gespeichert und anschließend unwiederbringlich gelöscht.

Wenn Sie auf Ihrem Gerät keine Code-Sperre eingerichtet haben, werden Sie nach 15 Minuten Inaktivität automatisch von "Freunde suchen" abgemeldet.

Weitere Informationen zu "Freunde suchen"

iCloud-Schlüsselbund

Verschlüsselungsschlüssel des iCloud-Schlüsselbunds werden auf Ihren Geräten erstellt, und Apple kann auf diese Schlüssel nicht zugreifen. Nur verschlüsselte Schlüsselbunddaten werden über die Server von Apple geleitet. Apple kann nicht auf die Schlüsselmaterialien zugreifen, die verwendet werden könnten, um die Daten zu entschlüsseln.

Nur von Ihnen genehmigte vertrauenswürdige Geräte können auf Ihren iCloud-Schlüsselbund zugreifen.

In den erweiterten Einstellungen können Sie einen iCloud-Sicherheitscode wählen, der mehr als vier Ziffern umfasst, oder Sie können das Gerät einen solchen für Sie generieren lassen.

Sie können wählen, die Schlüsselbundwiederherstellung zu deaktivieren. Dies bedeutet, dass der iCloud-Schlüsselbund auf allen genehmigten Geräten aktuell gehalten wird, aber dass die verschlüsselten Daten nicht bei Apple gespeichert werden und auch nicht wiederhergestellt werden können, wenn alle Ihre Geräte verloren gehen.

Fotos

Sie können jederzeit unerwünschte Fotos aus "Mein Fotostream" löschen. Hier erfahren Sie, wie Sie Ihre Fotos löschen.

Sie können jederzeit unerwünschte Fotos und Videos aus den freigegebenen Fotostreams löschen. Erfahren Sie, wie Sie Fotos und Videos aus einem freigegebenen Stream löschen.

Sie können Abonnenten jederzeit von freigegebenen Fotostreams, die Sie erstellt haben, entfernen. Erfahren Sie, wie Sie Abonnenten aus Ihrem freigegebenen Fotostream bewegen.

Erfahren Sie mehr über die iCloud-Fotofreigabe und "Mein Fotostream".