macOS Sicherheit

Überblick für die IT

Apple hat in seiner macOS Plattform Hardware, Software und Dienste integriert, die von Grund auf sicher sind und eine einfache Konfiguration, Implementierung und Verwaltung ermöglichen. macOS enthält die wichtigsten Sicherheitstechnologien, die IT-Fachkräfte benötigen, um Unternehmensdaten zu schützen und die Plattform in sichere unternehmensinterne Netzwerkumgebungen zu integrieren. Apple stellt zudem durch die Zusammenarbeit mit Normungsorganisationen sicher, dass die neuesten Sicherheitszertifizierungen erfüllt werden. In diesem Überblick stellen wir Ihnen einige dieser Funktionen vor.

Dieses Dokument ist in die folgenden Themenbereiche unterteilt:

- **Systemsicherheit:** Die integrierte, sichere Software, die die Grundlage von macOS bildet.
- **Verschlüsselung und Datenschutz:** Die Architektur und das Design, die Benutzerdaten schützen, falls das Gerät verloren geht oder gestohlen wird.
- **Sicherheit in Apps:** Die Systeme, die dafür sorgen, dass der Mac vor Malware geschützt ist und Apps sicher und ohne Gefährdung der Plattformintegrität ausgeführt werden können.
- **Authentifizierung und digitales Signieren:** Die in macOS integrierten Funktionen für die Zugangsdatenverwaltung und Unterstützung standardkonformer Technologien, wie z. B. Smart Cards und S/MIME.
- **Netzwerksicherheit:** Industriestandard-Netzwerkprotokolle, die eine sichere Authentifizierung und die Verschlüsselung von Daten bei der Übertragung ermöglichen.
- **Kontrollmechanismen für Geräte:** Methoden, die die Verwaltung von Apple Geräten erlauben, eine unbefugte Verwendung der Geräte verhindern und das Fernlöschen ermöglichen, falls ein Gerät verloren geht oder gestohlen wurde.

Weitere Informationen zur Implementierung und Verwaltung von macOS finden Sie in der Referenz zur macOS Implementierung unter help.apple.com/deployment/macos.

Weitere Informationen zu den Sicherheitsfunktionen der Apple Dienste, die nicht in diesem Dokument behandelt werden, finden Sie im „iOS Sicherheitshandbuch“ unter www.apple.com/de/business/docs/iOS_Security_Guide.pdf.

Systemsicherheit

Die macOS Systemsicherheit wurde so konzipiert, dass sowohl Software als auch Hardware über alle Kernkomponenten von jedem Mac hinweg sicher sind. Diese Architektur ist von zentraler Bedeutung für die Sicherheit in macOS, ohne dabei die Benutzerfreundlichkeit zu beeinträchtigen.

UNIX

Der macOS-Kernel – das Herz des Betriebssystems – basiert auf dem Berkeley Systems Distribution (BSD) und dem Mach-Mikrokernel. BSD stellt grundlegende Dateisystem- und Netzwerkdienste, ein Schema zur Identifizierung von Benutzern und Gruppen sowie viele weitere grundlegende Funktionen bereit. BSD setzt zudem Einschränkungen beim Zugriff auf Dateien und Systemressourcen durch, die auf Benutzer- und Gruppen-IDs basieren.

Mach liefert Speicherverwaltung, Thread-Kontrolle, Hardware-Abstraktion und Interprozesskommunikation. Mach-Ports repräsentieren Aufgaben und andere Ressourcen. Mach setzt den Zugriff auf die Ports durch die Kontrolle der Aufgaben um, die eine Nachricht an sie senden dürfen. BSD-Sicherheitsrichtlinien und Mach-Zugriffsberechtigungen bilden die wesentliche Grundlage der Sicherheit in macOS und spielen eine entscheidende Rolle bei der Durchsetzung der lokalen Sicherheit.

Die Sicherheit des Kernels ist für die Sicherheit des gesamten Betriebssystems wichtig. Codesignierung schützt den Kernel und Kernelerweiterungen von anderen Anbietern sowie andere von Apple entwickelte Systembibliotheken und ausführbare Programme.

Modell für Benutzerrechte

Ein wichtiger Aspekt der Mac Sicherheit ist das Erteilen oder Verweigern von Zugriffsberechtigungen, auch Zugriffsrechte genannt. Diese Rechte beziehen sich auf die Möglichkeit zum Ausführen eines konkreten Vorgangs, beispielsweise den Zugriff auf Daten oder das Ausführen von Code. Rechte werden auf der Ebene von Ordnern, Unterordnern, Dateien und Apps sowie für spezifische Daten in Dateien, für App-Funktionen und für Administrationsfunktionen gewährt. Digitale Signaturen identifizieren die Zugriffsrechte von Apps und Systemkomponenten.

macOS steuert Rechte auf vielen Ebenen, einschließlich der Mach- und BSD-Komponenten des Kernels. Zur Steuerung von Rechten für Apps im Netzwerk nutzt macOS Netzwerkprotokolle.

Obligatorische Zugriffssteuerung

macOS nutzt außerdem die obligatorische Zugriffssteuerung – Richtlinien, die vom Entwickler erstellte Sicherheitsbeschränkungen festlegen, die sich nicht umgehen lassen. Dieser Ansatz unterscheidet sich von einer frei wählbaren Zugriffssteuerung, bei der Benutzer Sicherheitsrichtlinien gemäß ihren Präferenzen außer Kraft setzen können. Die obligatorische Zugriffssteuerung können Benutzer nicht sehen. Es handelt sich bei ihr um die zugrundeliegende Technologie, die mehrere wichtige Funktionen ermöglicht, darunter Sandboxing, Kindersicherung, verwaltete Einstellungen, Erweiterungen und Systemintegritätsschutz.

Systemintegritätsschutz

OS X 10.11 und neuere Versionen enthalten den so genannten Systemintegritätsschutz, einen Schutz auf Systemebene, der einen Schreibschutz an bestimmten Speicherorten des Dateisystems festlegt, um Schadcode daran zu hindern, systemkritische Komponenten auszuführen oder zu modifizieren. Der Systemintegritätsschutz ist eine computerspezifische Einstellung, die beim Upgrade auf OS X 10.11 standardmäßig aktiviert ist. Wird er deaktiviert, geht der Schutz für alle Partitionen auf dem physischen Speichergerät verloren. macOS wendet diese Sicherheitsrichtlinie auf jeden Prozess an, der auf dem System ausgeführt wird. Dabei ist es irrelevant, ob er in einer Sandbox abgeschirmt oder mit Administratorrechten belegt wird.

Weitere Informationen zu diesen schreibgeschützten Bereichen des Dateisystems finden Sie im Apple Support Artikel „Informationen zum Systemintegritätsschutz auf dem Mac“ unter support.apple.com/HT204899.

Kernelerweiterungen

macOS bietet einen Mechanismus für Kernelerweiterungen, der das dynamische Laden von Code in den Kernel zulässt, ohne dass ein neues Kompilieren oder Verknüpfen nötig ist. Da diese Kernelerweiterungen (KEXTs) sowohl Modularität als auch dynamisches Laden mit sich bringen, sind sie die erste Wahl für jeden relativ eigenständigen Service, der auf interne Kernelschnittstellen zugreifen muss, zum Beispiel Hardware-Gerätetreiber oder VPN-Apps.

Um die Sicherheit auf dem Mac weiter zu verbessern, ist die Zustimmung des Benutzers erforderlich, um Kernelerweiterungen zu laden, die mit oder nach der Installation von macOS High Sierra installiert werden. Dies wird Laden von Kernelerweiterungen mit Benutzergenehmigung genannt. Jeder Benutzer kann eine Kernelerweiterung genehmigen, auch wenn er keine Administratorrechte besitzt.

In den folgenden Fällen erfordern Kernelerweiterungen keine Autorisierung:

- Sie waren schon vor dem Upgrade auf MacOS High Sierra auf dem Mac installiert.
- Sie ersetzen zuvor genehmigte Erweiterungen.
- Sie dürfen ohne Benutzergenehmigung geladen werden, da beim Start mit der macOS Wiederherstellung der Befehl `spctl` verwendet wird.
- Sie dürfen über die Konfiguration zur mobilen Geräteverwaltung (Mobile Device Management, MDM) geladen werden. Beginnend mit macOS High Sierra 10.13.2 können Sie MDM verwenden, um eine Liste von Kernelerweiterungen festzulegen, die auch ohne Benutzergenehmigung geladen werden dürfen. Diese Option erfordert einen Mac mit macOS High Sierra 10.13.2, der entweder über das Programm zur Geräteregistrierung (Device Enrollment Programm, DEP) bei MDM registriert ist oder dessen Registrierung bei MDM vom Benutzer genehmigt wurde.

Weitere Informationen zu Kernelerweiterungen finden Sie im Apple Support Artikel „Auf Änderungen an Kernelerweiterungen in macOS High Sierra vorbereiten“ unter support.apple.com/HT208019.

Firmware-Passwort

macOS unterstützt die Verwendung eines Passworts, um unbeabsichtigte Änderungen an den Firmware-Einstellungen auf einem bestimmten System zu verhindern. Mit diesem Firmware-Passwort verhindern Sie Folgendes:

- Starten von einem unautorisierten Systemvolume
- Veränderung des Startvorgangs, zum Beispiel Starten im Einzelbenutzermodus
- Unautorisierter Zugriff auf die macOS Wiederherstellung
- Direkter Speicherzugriff (Direct Memory Access, DMA) über Schnittstellen wie Thunderbolt
- Festplattenmodus, der DMA erfordert

Anmerkung: Der Apple T2 Chip im iMac Pro verhindert, dass Benutzer das Firmware-Passwort zurücksetzen können, selbst wenn sie physischen Zugriff auf den Mac haben. Bei einem Mac ohne T2 Chip müssen zusätzliche Vorsichtsmaßnahmen ergriffen werden, um den physischen Zugriff durch Benutzer auf die internen Mac-Komponenten zu verhindern.

Internetwiederherstellung

Mac Computer versuchen automatisch, über das Internet einen Start aus macOS Wiederherstellung durchzuführen, wenn ein Start über das integrierte

Wiederherstellungssystem nicht möglich ist. In solch einem Fall wird Ihnen beim Starten anstelle des Apple Logos eine sich drehende Weltkugel angezeigt. Mit der Internetwiederherstellung kann ein Benutzer die neueste macOS Version oder die mit seinem Mac gelieferte Version neu installieren.

macOS Updates werden über den App Store verteilt und vom macOS Installationsprogramm durchgeführt, das mithilfe von Codesignaturen die Integrität und Authentizität des Installationsprogramms und seiner Pakete vor der Installation sicherstellt. Genauso ist die Internetwiederherstellung die autoritative Quelle für das Betriebssystem, das mit einem bestimmten Mac geliefert wurde.

Weitere Informationen zur macOS Wiederherstellung finden Sie im Apple Support Artikel „Informationen zu macOS Wiederherstellung" unter support.apple.com/HT201314.

Verschlüsselung und Datenschutz

Apple Dateisystem

Das Apple Dateisystem (Apple File System, APFS) ist ein neues, modernes Dateisystem für macOS, iOS, tvOS und watchOS. Es wurde für Flash-/SSD-Speicher optimiert. Seine Leistungsmerkmale sind starke Verschlüsselung, Copy-on-Write-Metadaten, Freigeben und Teilen von Speicherplatz, Klonen von Dateien und Verzeichnissen, Schnappschüsse, schnelle Verzeichnisdimensionierung, Atomic Safe-Save-Speicherfunktionen, allgemeine Verbesserungen des Dateisystems sowie ein einzigartiges Copy-on-Write-Design, das I/O Coalescing nutzt, um maximale Leistung und Datensicherheit zu gewährleisten.

APFS weist Speicherplatz bedarfsgesteuert zu. Wenn ein einzelner APFS Container mehrere Volumes enthält, wird der freie Speicherplatz des Containers geteilt und kann bei Bedarf jedem der einzelnen Volumes zugewiesen werden. Jedes Volume nutzt nur einen Teil des gesamten Containers. Der verfügbare Speicherplatz entspricht damit der Gesamtgröße des Containers abzüglich des Speicherplatzes, der in allen Volumens des Containers belegt wird.

Für macOS High Sierra muss ein gültiger APFS Container mindestens drei Volumes enthalten (die ersten beiden werden dem Benutzer nicht angezeigt):

- Preboot-Volume: Enthält Daten, die für das Starten jedes Systemvolumes im Container benötigt werden.
- Wiederherstellungsvolume: Enthält die Recovery Disk.
- Systemvolume: Enthält macOS und den Benutzerordner.

FileVault

Jeder Mac besitzt eine integrierte Verschlüsselung namens FileVault, um alle gespeicherten Daten zu schützen. Für den Schutz der auf einem Mac gespeicherten Daten nutzt FileVault die Datenverschlüsselung XTS-AES-128. Sie kann für den gesamten Volumenschutz auf internen Festplatten und Wechseldatenträgern angewendet werden. Wenn ein Benutzer im Systemassistenten eine Apple ID und ein Passwort eingibt, empfiehlt der Assistent die Aktivierung von FileVault und das Speichern des Wiederherstellungsschlüssels in iCloud.

Ein Benutzer, der FileVault auf einem Mac aktiviert, wird aufgefordert, gültige Anmeldedaten einzugeben, bevor der Startvorgang fortgesetzt wird. Zudem erhält er so Zugriff auf spezielle Startmodi wie den Festplattenmodus. Ohne gültige Anmeldedaten oder einen Wiederherstellungsschlüssel bleibt das gesamte Volume verschlüsselt und ist vor unbefugten Zugriffen geschützt. Dies gilt selbst dann, wenn das physische Speichergerät entfernt und mit einem anderen Computer verbunden wird.

Für den Schutz von Unternehmensdaten sollte die IT Konfigurationsrichtlinien für FileVault definieren und über MDM durchsetzen. Unternehmen haben mehrere Möglichkeiten für die Verwaltung verschlüsselter Volumes, einschließlich institutioneller Wiederherstellungsschlüssel, persönlicher Wiederherstellungsschlüssel (die optional mit MDM für die Schlüsselverwahrung gespeichert werden können) oder einer Kombination beider Optionen. Die Schlüsselrotation kann ebenfalls als Richtlinie in MDM festgelegt werden.

Verschlüsselte Images

In macOS dienen verschlüsselte Images als sichere Container, die der Benutzer nutzen kann, um sensible Dokumente und andere Dateien zu speichern und zu übertragen. Verschlüsselte Images werden mit dem Festplattendienstprogramm erstellt, das Sie unter /Programme/Dienstprogramme/ finden. Images können mit 128-Bit- oder 256-Bit-AES-Verschlüsselung geschützt werden. Da ein aktiviertes Image als lokales, mit einem Mac verbundenes Volume behandelt wird, können Benutzer die darin gespeicherten Dateien und Ordner kopieren, bewegen und öffnen. Wie bei FileVault werden die Inhalte eines Images in Echtzeit ver- und entschlüsselt. Bei verschlüsselten Images können Benutzer Dokumente, Dateien und Ordner sicher austauschen, indem sie ein verschlüsseltes Image auf einem Wechseldatenträger speichern, als Anhang einer E-Mail senden oder auf einem externen Server speichern.

Zertifizierung nach ISO-Normen 27001 und 27018

Das Managementsystem zur Informationssicherheit (Information Security Management System, ISMS) von Apple zur Gewährleistung der Sicherheit von Infrastruktur, Entwicklung und Betrieb ist für die folgenden Produkte und Dienstleistungen nach den ISO-Normen 27001 und 27018 zertifiziert: Apple School Manager, iCloud, iMessage, FaceTime, verwaltete Apple IDs und iTunes U, entsprechend der Anwendbarkeitserklärung Version 2.1 vom 11. Juli 2017. Die bestehende Konformität mit der ISO-Norm wurde Apple durch die British Standards Institution (BSI) zertifiziert. Diese Konformitätszertifikate für ISO 27001 und ISO 27018 sind auf der Website der BSI verfügbar:

www.bsigroup.com/de-DE/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/de-DE/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Cryptographic Validation (FIPS 140-2)

Seit OS X 10.6 wird die Konformität der kryptografischen Module in macOS mit den U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1 nach jeder neuen Version validiert. Mit jeder neuen Version reicht Apple die Module zur Revalidierung beim CMVP (Cryptographic Module Validation Program) ein, bevor eine neue Version des Mac Betriebssystems veröffentlicht wird. Dieses Programm validiert die Integrität kryptografischer Funktionen für Apple Apps und Apps von anderen Anbietern, die die kryptografischen Dienste und anerkannten Algorithmen in macOS ordnungsgemäß nutzen. Alle Validierungszertifikate zur Konformität von Apple mit FIPS 140-2 finden Sie auf der CMVP-Anbieterseite. Das CMVP führt den Validierungsstatus kryptografischer Module je nach Bearbeitungsstand in zwei unterschiedlichen Listen unter csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Common Criteria Certification (ISO 15408)

Apple hat bereits Zertifizierungen für macOS im Rahmen des Zertifizierungsprogramms nach Common Criteria erhalten und beteiligt sich erneut an einer Bewertung von macOS High Sierra anhand von Schutzprofilen für Betriebssysteme (Operating System Protection Profiles) (PP_OSv4.1).

Apple wird auch weiterhin Beurteilungen nach neuen und aktualisierten Versionen der heute verfügbaren international abgestimmten Schutzprofile (collaborative Protection Profiles, cPPs) durchführen und entsprechende Zertifizierungen anstreben. Apple nimmt eine aktive Rolle innerhalb der International Technical Community (ITC) bei der Entwicklung von cPP ein, die sich auf die Evaluierung wichtiger mobiler Sicherheitstechnologie konzentrieren.

Sicherheitszertifizierungen, -programme und -empfehlungen

Apple hat gemeinsam mit den staatlichen Behörden verschiedenster Länder Leitfäden entwickelt, in denen Vorgehensweisen und Empfehlungen für die Gewährleistung einer sicheren Umgebung festgehalten sind, auch bekannt als „Härtung des Geräts" (Device Hardening) für Hochrisikoumgebungen. Diese Leitfäden enthalten sorgsam definierte und geprüfte Informationen darüber, wie Features in macOS im Interesse eines verbesserten Schutzes konfiguriert und verwendet werden können.

Die neuesten Informationen zu macOS Sicherheitszertifizierungen, -validierungen und -empfehlungen finden Sie im Apple Support Artikel „Zertifizierungen, Validierungen und Empfehlungen zur Produktsicherheit für macOS" unter support.apple.com/HT201159.

Sicherheit in Apps

Integrierte Technologien in macOS sorgen dafür, dass nur Apps aus vertrauenswürdigen Quellen installiert werden, und bieten Schutz vor Malware. Um sicherzustellen, dass Apps nicht manipuliert werden können, verwendet macOS ein mehrstufiges Sicherheitskonzept für den Laufzeitschutz und die Signierung von Apps.

Gatekeeper

macOS bietet ein Feature namens Gatekeeper, um die Quellen zu kontrollieren, von denen Apps installiert werden können. Mit Gatekeeper können Benutzer und Unternehmen ein für die Installation von Apps erforderliches Sicherheitsniveau festlegen.

Mit der sichersten Gatekeeper-Einstellung können Benutzer nur signierte Apps aus dem App Store installieren. Die Standardeinstellung ermöglicht Benutzern, Apps aus dem App Store und Apps mit gültiger Entwickler-ID-Signatur zu installieren. Diese Signatur zeigt an, dass die Apps mit einem von Apple ausgestellten Zertifikat signiert und seitdem nicht verändert wurden. Gatekeeper kann bei Bedarf über einen Terminal-Befehl auch komplett deaktiviert werden.

Außerdem wendet Gatekeeper in einigen Fällen eine Pfadrandomisierung an. Dies gilt auch für Apps, die direkt von einem unsignierten Image oder von dem Speicherort gestartet werden, in den sie geladen und in dem sie automatisch entpackt wurden. Die Pfadrandomisierung stellt Apps vor dem Starten von einem nicht spezifizierten schreibgeschützten Speicherort im Dateisystem zur Verfügung. So wird verhindert, dass Apps über relative Pfade auf Codes oder Inhalte zugreifen oder sich selbst aktualisieren, wenn sie von diesem schreibgeschützten Speicherort aus gestartet werden. Wenn eine App mithilfe des Finders beispielsweise in den Ordner „Programme“ verschoben wird, wird die Pfadrandomisierung nicht länger angewendet.

Der größte Vorteil des standardmäßigen Sicherheitsmodells ist, dass es einen umfassenden Schutz des Ökosystems bietet. Falls es ein Malware-Verursacher schafft, an die Entwickler-ID-Signatur zu gelangen und diese für die Verteilung von Malware zu verwenden, kann Apple schnell reagieren, indem es das Signaturzertifikat annulliert. So wird die weitere Verbreitung der Malware unterbunden. Diese Sicherungen sorgen dafür, dass das Wirtschaftsmodell der meisten Malware-Kampagnen auf dem Mac unterwandert wird und alle Benutzer umfassend geschützt sind.

Benutzer können diese Einstellungen vorübergehend außer Kraft setzen und jede App installieren. Unternehmen können ihre MDM-Lösung verwenden, um Gatekeeper Einstellungen zu definieren und durchzusetzen. Außerdem können sie Zertifikate zur macOS Vertrauensrichtlinie hinzufügen, um die Codesignierung zu evaluieren.

XProtect

macOS enthält eine integrierte Technologie für die signaturbasierte Malware-Erkennung. Apple hält nach neuen Malware-Infektionen und Viren Ausschau und aktualisiert automatisch die XProtect Signaturen – unabhängig von den Systemupdates –, um Mac Systeme vor Malware-Infektionen zu schützen. XProtect erkennt und blockiert automatisch die Installation von bekannter Malware.

Malware-Removal-Tool

Sollte sich Malware ihren Weg auf einen Mac bahnen, verfügt macOS auch über eine Technologie zur Beseitigung von Infektionen. Apple überwacht aber nicht nur die Malware-Aktivität im Ökosystem, um Entwickler-IDs (sofern zutreffend) zu annullieren und XProtect Updates zu veröffentlichen, sondern gibt auch Updates für macOS heraus, um Malware von betroffenen Systemen zu

entfernen, die für den Empfang automatischer Sicherheitsupdates konfiguriert wurden. Sobald das Malware-Removal-Tool aktualisierte Informationen erhalten hat, wird die Malware nach dem nächsten Neustart entfernt. Das Malware-Removal-Tool startet den Mac nicht automatisch neu.

Automatische Sicherheitsupdates

Apple veröffentlicht die Updates für XProtect und das Malware-Removal-Tool automatisch. Standardmäßig sucht macOS täglich nach diesen Updates. Weitere Informationen zu automatischen Sicherheitsupdates finden Sie im Apple Support Artikel „Mac App Store: Automatische Sicherheitsupdates“ unter support.apple.com/HT204536.

Laufzeitschutz

Systemdateien, Ressourcen und der Kernel werden vom App-Bereich eines Benutzers abgeschirmt. Alle Apps aus dem App Store laufen in einer Sandbox, um den Zugriff auf Daten zu schützen, die von anderen Apps gespeichert werden. Muss eine App vom App Store auf die Daten einer anderen App zugreifen, ist dies nur mit den von macOS bereitgestellten APIs und Diensten möglich.

Zwingende Codesignierung von Apps

Alle Apps aus dem App Store werden von Apple signiert, um sicherzustellen, dass sie nicht manipuliert oder verändert wurden. Apple signiert alle Apps, die auf Apple Geräten vorinstalliert sind. Viele außerhalb des App Store verteilte Apps werden vom Entwickler mit einem von Apple ausgegebenen Entwickler-ID-Zertifikat (in Kombination mit einem privaten Schlüssel) signiert, um unter den Standardeinstellungen von Gatekeeper ausgeführt werden zu können.

Apps von außerhalb des App Store sind in der Regel ebenfalls mit einem von Apple ausgegebenen Entwicklerzertifikat signiert. So können Sie überprüfen, ob die App authentisch ist und nicht manipuliert wurde. Intern entwickelte Apps müssen ebenfalls mit einer von Apple ausgegebenen Entwickler-ID signiert werden, damit Sie ihre Integrität validieren können.

Die obligatorische Zugangssteuerung (Mandatory Access Control, MAC) erfordert die Codesignierung, um vom System geschützte Berechtigungen zu aktivieren. Apps beispielsweise, die einen Zugang durch die Firewall erfordern, müssen mit der entsprechenden MAC-Berechtigung mit Code signiert werden.

Authentifizierung und digitales Signieren

Für die bequeme, sichere Speicherung von Zugangsdaten und digitalen Identitäten der Benutzer umfasst macOS den Schlüsselbund und andere Tools, die Technologien für das Authentifizieren und digitale Signieren unterstützen, zum Beispiel Smart Cards und S/MIME.

Schlüsselbund-Architektur

macOS bietet mit dem so genannten Schlüsselbund einen praktischen und sicheren Speicherort für Anmeldedaten, einschließlich digitaler Identitäten, Verschlüsselungsschlüssel und sicherer Notizen. Er ist über die App „Schlüsselbundverwaltung“ im Ordner /Programme/Dienstprogramme/ zugänglich. Durch das Verwenden eines Schlüsselbunds muss ein Benutzer die Anmeldedaten für verschiedene Ressourcen nicht mehr einzeln eingeben und sich nicht einmal mehr daran erinnern. Ein erster Standardschlüsselbund wird für jeden Mac Benutzer erstellt. Benutzer können jedoch weitere zusätzliche Schlüsselbunde für bestimmte Zwecke hinzufügen.

Neben den Schlüsselbunden der Benutzer verwendet macOS auf Systemebene eine Reihe von Schlüsselbunden für die Verwaltung von Authentifizierungsdaten, die nicht benutzerspezifisch sind. Hierzu gehören Anmeldedaten für das Netzwerk und Zertifikate für öffentliche Schlüssel (Public Key Infrastructure, PKI).

Einer dieser Schlüsselbunde, System-Roots, ist unveränderbar und stellt Internet-PKI-Root-Zertifikate über eine interne Root-Zertifizierungsstelle bereit, die allgemeine Aufgaben wie Online-Banking und E-Commerce ermöglichen. Ähnlich können Sie Zertifikate über eine interne Zertifizierungsstelle für verwaltete Mac Computer bereitstellen, damit sie sich bei internen Sites und Diensten anmelden können.

Sicheres Authentifizierungs-Framework

Die Daten im Schlüsselbund werden durch Zugriffssteuerungslisten (Access Control Lists, ACLs) partitioniert und geschützt, sodass Anmeldedaten, die in Apps anderer Anbieter gespeichert sind, ohne ausdrückliche Zustimmung des Benutzers nicht von anderen Apps eingesehen werden können. Dieser Schutzmechanismus schützt die Authentifizierungs- und Anmeldedaten unterschiedlicher Apps und Dienste auf Apple Geräten innerhalb Ihres Unternehmens.

Touch ID

Mac Systeme mit einem Touch ID Sensor können per Fingerabdruck entsperrt werden. Touch ID ersetzt nicht das Passwort. Dieses ist weiterhin erforderlich, um sich nach dem Start, Neustart oder Abmelden auf einem Mac anzumelden. Nach der Anmeldung können sich Benutzer schnell mit Touch ID authentifizieren, wenn sie nach einem Passwort gefragt werden.

Benutzer können mit Touch ID außerdem durch ein Passwort geschützte Notizen in der Notizen App, den Bereich „Passwörter" in den Safari Einstellungen sowie weitere Einstellungsseiten in den Systemeinstellungen öffnen. Um die Sicherheit zu erhöhen, müssen Benutzer ein Passwort eingeben und können nicht Touch ID verwenden, wenn sie den Bereich „Sicherheit" in den Systemeinstellungen öffnen wollen. Wenn FileVault aktiviert ist, müssen Benutzer ebenfalls ein Passwort eingeben, um die Einstellungen für „Benutzer & Gruppen" zu verwalten. Mehrere Benutzer, die sich auf dem gleichen Mac anmelden, können mit Touch ID bequem das Benutzerkonto wechseln.

Weitere Informationen zu Touch ID und seiner Sicherheit finden Sie im Apple Support Artikel „Informationen zur fortschrittlichen Sicherheitstechnologie von Touch ID" unter support.apple.com/HT204587.

Automatisches Entsperren mit der Apple Watch

Benutzer können mit ihrer Apple Watch automatisch ihren Mac entsperren. Bluetooth Low Energy (BLE) und Peer-to-Peer-WLAN sorgen dafür, dass die Apple Watch einen Mac sicher entsperren kann, wenn sich beide Geräte in unmittelbarer Nähe zueinander befinden. Dafür wird ein iCloud Konto mit konfigurierter Zwei-Faktor-Authentifizierung benötigt.

Details zum Protokoll sowie weitere Informationen zu den Funktionen Integration und Handoff finden Sie im „iOS Sicherheitshandbuch" unter www.apple.com/de/business/docs/iOS_Security_Guide.pdf.

Smart Cards

macOS Sierra und neuer bietet native Unterstützung für PIV-Karten (Personal Identity Verification). Diese Karten sind in der Industrie und bei Behörden weit verbreitet und werden für die Zwei-Faktor-Authentifizierung, für digitale Signaturen und für die Verschlüsselung verwendet.

Smart Cards beinhalten eine oder mehrere digitale Identitäten mit jeweils einem öffentlichen und einem privaten Schlüssel und dem zugehörigen Zertifikat. Das Entsperren mithilfe der persönlichen Identifikationsnummer (PIN) gibt den Zugriff auf die privaten Schlüssel frei, die für die Authentifizierung, die Verschlüsselung und/oder das Signieren verwendet werden. Das Zertifikat bestimmt, für welche Zwecke der Schlüssel verwendet werden kann und welche

Attribute ihm zugeordnet sind. Außerdem gibt es an, ob es durch eine Zertifizierungsstelle validiert (signiert) wurde.

Smart Cards können für die Zwei-Faktor-Authentifizierung verwendet werden. Die beiden Faktoren sind ein „Objekt, das Sie haben" (die Karte) und eine „Information, die Sie wissen" (die PIN). macOS Sierra und neuere Versionen bieten native Unterstützung für Smart Cards als Mittel für die Authentifizierung im Anmeldefenster und für die zertifikatbasierte Authentifizierung gegenüber Websites in Safari. Außerdem unterstützt macOS die Kerberos-Authentifizierung mithilfe eines Schlüsselpaars (PKINIT) für die Einmalanmeldung bei Diensten, die Kerberos unterstützen.

Weitere Informationen zur Smart-Card-Implementierung mit macOS finden Sie in der Referenz zur macOS Implementierung unter help.apple.com/deployment/macos.

Digitale Signaturen und Verschlüsselung

In der Mail App können Benutzer digital signierte und verschlüsselte Nachrichten senden. Bei kompatiblen Smart Cards erkennt die App Mail in den digitalen Signatur- und Verschlüsselungszertifikaten der PIV-Token automatisch die nach Groß- und Kleinschreibung unterschiedenen Namen oder Alternativnamen des Inhabers einer E-Mail-Adresse (RFC822). Wenn eine konfigurierte E-Mail-Adresse mit einer E-Mail-Adresse im digitalen Signatur- oder Verschlüsselungszertifikat des PIV-Token übereinstimmt, zeigt Mail in einer neuen Symbolleiste automatisch die Taste zum Signieren der E-Mail an. Wenn Mail über das Zertifikat des Empfängers für die Verschlüsselung von E-Mails verfügt oder dieses in der globalen Adressliste (Global Address List, GAL) von Microsoft Exchange finden kann, wird in der neuen Symbolleiste ein Schloss-Symbol angezeigt. Das Schloss-Symbol signalisiert, dass die Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und in dieser Form gesendet wird.

S/MIME auf E-Mail-Basis

macOS unterstützt das Erstellen von S/MIME auf der Ebene einzelner Nachrichten. Das bedeutet, dass S/MIME-Benutzer bestimmen können,ob sie E-Mails standardmäßig immer signieren und verschlüsseln oder selektiv einzelne E-Mails signieren und verschlüsseln möchten.

Zertifikate für die Verwendung mit S/MIME können via Konfigurationsprofil, MDM-Lösung, Simple Certificate Enrollment Protocol (SCEP) oder Microsoft Active Directory Zertifizierungsstelle an Apple Geräte übermittelt werden.

Netzwerksicherheit

Zusätzlich zu den integrierten Sicherheitsmaßnahmen, die Apple zum Schutz der auf dem Mac gespeicherten Daten verwendet, gibt es viele Netzwerksicherheitsmaßnahmen, die Unternehmen ergreifen können, damit Informationen bei der Übertragung an und von einem Mac sicher bleiben.

Mobile Benutzer müssen von überall auf der Welt auf Unternehmensnetzwerke zugreifen können. Daher muss sichergestellt werden, dass sie über die entsprechenden Zugriffsrechte verfügen und ihre Daten während der Übertragung zuverlässig geschützt sind. macOS nutzt – und bietet Entwicklern Zugriff auf – Standardnetzwerkprotokolle für die authentifizierte, autorisierte und verschlüsselte Kommunikation. Um diese Sicherheitsziele zu erreichen, nutzt macOS bewährte Technologien und die aktuellsten Standards für WLAN-Datenverbindungen.

TLS

macOS unterstützt Transport Layer Security (TLS 1.0, TLS 1.1 und TLS 1.2) und DTLS. Es unterstützt sowohl AES-128 als auch AES-256 und bevorzugt Chiffrensammlungen (Cipher Suites) mit Perfect Forward Secrecy. Safari,

Kalender, Mail und andere Internet-Apps verwenden diese Protokolle automatisch, um einen verschlüsselten Kommunikationskanal zwischen dem Gerät und Netzwerkdiensten sicherzustellen.

High-Level-APIs (wie CFNetwork) erleichtern es Entwicklern, TLS für ihre Apps zu verwenden. Im Gegensatz dazu bieten Low-Level-APIs (wie SecureTransport) präzise Einstellungsmöglichkeiten. CFNetwork lässt SSLv3 nicht zu und Apps, die vom WebKit Gebrauch machen (z. B. Safari), können keine SSLv3-Verbindung herstellen.

Ab macOS High Sierra und iOS 11 sind SHA-1-Zertifikate für TLS-Verbindungen nicht länger zulässig, sofern der Benutzer ihnen nicht vertraut. Zertifikate mit RSA-Schlüsseln, die weniger als 2048 Bits haben, sind ebenfalls nicht erlaubt. Die RC4-Cipher-Suite für die symmetrische Verschlüsselung findet in macOS Sierra und iOS 10 keine Anwendung. Standardmäßig sind RC4-Cipher-Suites auf TLS-Clients oder -Servern, die mit SecureTransport-APIs implementiert wurden, nicht aktiviert und können keine Verbindung herstellen, wenn es sich bei RC4 um die einzige verfügbare Chiffrensammlung handelt. Um für mehr Sicherheit zu sorgen, müssen Dienste und Apps, die RC4 benötigen, so aktualisiert werden, dass moderne, sichere Chiffrensammlungen genutzt werden.

App Transport Security

App Transport Security umfasst Anforderungen für Standardverbindungen, um bei Verwendung von NSURLConnection-, CFURL- oder NSURLSession-APIs sicherzustellen, dass Apps die bewährten Verfahren für sichere Verbindungen einhalten. Standardmäßig beschränkt App Transport Security die Cipher-Auswahl ausschließlich auf Chiffrensammlungen, die Forward Secrecy bereitstellen, insbesondere ECDHE_ECDSA_AES und ECDHE_RSA_AES im GCM- oder CBC-Modus. Apps sind in der Lage, die Forward-Secrecy-Erfordernis pro Domain zu deaktivieren. In diesem Fall wird RSA_AES zur Gruppe der verfügbaren Ciphern hinzugefügt.

Server müssen TLS 1.2 und Forward Secrecy unterstützen und Zertifikate müssen auf der Basis von SHA-256 (oder neuer) validiert und signiert sein, wobei ein 2048-Bit-RSA-Schlüssel oder ein 256-Bit-ECC-Schlüssel (elliptischer Kurven-Schlüssel) die Mindestanforderung darstellt.

Netzwerkverbindungen, die diese Anforderungen nicht erfüllen, kommen nicht zustande, es sei denn, die Apps setzt die in App Transport Security definierten Anforderungen für die Transportsicherheit außer Kraft. Ungültige Zertifikate führen in jedem Fall zu einem nicht behebbaren Fehler (Hard Failure) und zum Nichtzustandekommen der Verbindung. App Transport Security wird automatisch auf die Apps angewendet, die für macOS 10.11 oder neuer kompiliert werden.

VPN

Die Einbindung sicherer Netzwerkdienste wie VPN (Virtual Private Network) in macOS erfordert nur minimalen Einrichtungs- und Konfigurationsaufwand. Mac Computer funktionieren mit VPN-Servern, die die folgenden Protokolle und Authentifizierungsmethoden unterstützen:

- IKEv2/IPSec mit Authentifizierung per Shared Secret (gemeinsam genutzter Schlüssel), RSA-Zertifikaten, ECDSA-Zertifikaten, EAP-MSCHAPv2 oder EAP-TLS
- SSL-VPN mit der jeweiligen Client-App aus dem App Store
- Cisco IPSec mit Benutzerauthentifizierung per Passwort, RSA SecurID oder CRYPTOCard sowie Systemauthentifizierung mittels Shared Secret und Zertifikaten
- L2TP/IPSec mit Benutzerauthentifizierung per Passwort (MS-CHAPv2), RSA SecurID oder CRYPTOCard sowie Systemauthentifizierung mittels Shared Secret

Neben den VPN-Lösungen anderer Anbieter unterstützt macOS die folgenden Lösungen:

- **VPN On Demand** für Netzwerke, die eine zertifikatbasierte Authentifizierung verwenden. IT-Richtlinien legen fest, für welche Domains eine VPN-Verbindung mit einem VPN-Konfigurationsprofil erforderlich ist.
- **VPN pro App**, mit dem sich VPN-Verbindungen noch detaillierter und präziser einstellen lassen. Über MDM können Kunden für jede verwaltete App und bestimmte Domains in Safari Verbindungen festlegen. So wird sichergestellt, dass nur sichere Daten vom und zum Unternehmensnetzwerk übertragen werden – die persönlichen Daten eines Benutzers jedoch nicht.

WLAN

macOS unterstützt die Branchenstandards für WLAN-Protokolle, darunter WPA2 Enterprise, um einen authentifizierten Zugriff auf drahtlose Unternehmensnetzwerke bereitzustellen. WPA2 Enterprise nutzt die 128-Bit-AES-Verschlüsselung und bietet den Benutzern so die größte Sicherheit dafür, dass ihre Daten geschützt bleiben, wenn sie Informationen über eine WLAN-Verbindung senden und empfangen. Da Mac Computer den Standard 802.1X unterstützen, können sie in eine Vielzahl von RADIUS-Authentifizierungsumgebungen integriert werden. Methoden für die drahtlose 802.1X-Authentifizierung umfassen EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 und LEAP.

Sie können die Authentifizierung für WPA/WPA2 Enterprise-Netzwerke auch im Anmeldefenster von macOS verwendet werden. Der Benutzer meldet sich dann an, um sich für das Netzwerk zu authentifizieren.

Der macOS Systemassistent nutzt 802.1X-Authentifizierung mit Benutzername und Passwort über TTLS oder PEAP.

Firewall

macOS umfasst eine integrierte Firewall, die den Mac vor Netzwerkzugriffen und Denial-of-Service-Angriffen schützt. Sie unterstützt die folgenden Konfigurationen:

- Alle eingehenden Verbindungen blockieren, unabhängig von der App
- Integrierter Software automatisch erlauben, eingehende Verbindungen zu empfangen
- Geladener signierter Software automatisch erlauben, eingehende Verbindungen zu empfangen
- Den Zugriff basierend auf vom Benutzer festgelegten Apps erlauben oder verweigern
- Verhindern, dass der Mac auf ICMP-Prüfanfragen und Portscan-Anfragen antwortet

Einmalanmeldung

macOS unterstützt die Authentifizierung mit Kerberos für Unternehmensnetzwerke. Apps können Kerberos verwenden, um Benutzer für Dienste zu authentifizieren, auf die sie zugreifen dürfen. Kerberos kann auch für eine Reihe verschiedener Netzwerkaktivitäten verwendet werden, zum Beispiel in sicheren Safari-Sitzungen und für die Authentifizierung von Drittanbieter-Apps beim Netzwerkdateisystem. Die zertifikatbasierte Authentifizierung (PKINIT) wird ebenfalls unterstützt, jedoch muss die App eine Entwickler-API verwenden.

GSS-API SPNEGO Token und das HTTP Negotiate Protokoll funktionieren mit Kerberos-basierten Authentifizierungsgateways und Windows Integrated Authentication Systemen, die Kerberos-Tickets unterstützen. Die Kerberos-Unterstützung basiert auf dem Open-Source-Projekt Heimdal.

Die folgenden Verschlüsselungstypen werden unterstützt:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1

- ARCFOUR-HMAC-MD5

Für die Konfiguration von Kerberos erwerben Sie Tickets mit Ticket Viewer, melden sich bei einer Windows Active Directory Domain an oder verwenden das Befehlszeilenprogramm `kinit`.

Sicherheit bei AirDrop

Mac Computer mit AirDrop Unterstützung verwenden Bluetooth Low Energy (BLE) und von Apple entwickelte Peer-to-Peer-WLAN-Technologien, um Dateien und Informationen auf Geräte in der Nähe zu senden, zu denen auch AirDrop fähige iOS Geräte mit iOS 7 oder neuer gehören. Die Geräte kommunizieren direkt per WLAN-Funk miteinander, ohne dass eine Internetverbindung oder ein WLAN-Zugangspunkt benötigt wird. Diese Verbindung wird mit TLS verschlüsselt.

Weitere Informationen zu AirDrop, Sicherheit bei AirDrop und anderen Apple Diensten finden Sie im Abschnitt „Netzwerksicherheit" im „iOS Sicherheitshandbuch" unter www.apple.com/de/business/docs/iOS_Security_Guide.pdf.

Kontrollmechanismen für Geräte

macOS unterstützt flexible Sicherheitsrichtlinien und Konfigurationen, die einfach durchzusetzen und zu verwalten sind. So können Unternehmen ihre Daten schützen und sicherstellen, dass Mitarbeiter die Unternehmensanforderungen erfüllen, auch wenn sie Computer nutzen, die sie selbst mitgebracht haben – zum Beispiel im Rahmen eines BYOD-Programms (Bring Your Own Device).

Unternehmen können Ressourcen wie Passwortschutz, Konfigurationsprofile und MDM-Lösungen von anderen Anbietern nutzen, um ihre Geräte zu verwalten und dafür zu sorgen, dass Unternehmensdaten sicher bleiben, auch wenn Mitarbeiter auf ihren persönlichen Mac Computern auf diese Daten zugreifen.

Passwortschutz

Auf Mac Computern mit Touch ID beträgt die Mindestlänge für Codes acht Zeichen. Lange und komplizierte Passwörter sind immer empfehlenswert, da sie nicht so einfach zu erraten oder anzugreifen sind.

Administratoren können komplexe Passwörter und andere Richtlinien mit MDM durchsetzen oder von Benutzern verlangen, Konfigurationsprofile manuell zu installieren. Sie benötigen ein Administratorpasswort, um die Payload „Code" in macOS zu installieren.

Weitere Informationen zu jeder in den MDM-Einstellungen verfügbaren Richtlinie finden Sie unter help.apple.com/deployment/mdm/#/mdm4D6A472A.

Entwickler finden weitere Informationen zu jeder Richtlinie im Dokument „Configuration Profile Reference" unter developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Durchsetzung von Konfigurationen

Ein Konfigurationsprofil ist eine XML-Datei, die es einem Administrator ermöglicht, Konfigurationsdaten an Mac Computer zu verteilen. Wenn der Benutzer ein Konfigurationsprofil löscht, werden alle vom Profil definierten Einstellungen ebenfalls entfernt. Administratoren können Einstellungen durchsetzen, indem sie Richtlinien mit dem WLAN- und Datenzugriff verknüpfen. So kann zum Beispiel ein Konfigurationsprofil, das eine E-Mail-Konfiguration enthält, auch eine Coderichtlinie vorgeben. Ein Benutzer kann erst auf seine E-Mails zugreifen, wenn das Passwort die Anforderungen des Administrators erfüllt.

Ein macOS Konfigurationsprofil enthält eine Reihe von Einstellungen, die festgelegt werden können, zum Beispiel:

- Coderichtlinien
- Beschränkungen von Gerätefunktionen (z. B. die Kamera deaktivieren)
- WLAN- oder VPN-Einstellungen
- Einstellung für Mail oder Exchange Server
- Einstellungen für den LDAP-Verzeichnisdienst
- Firewall-Einstellungen
- Anmeldedaten und Schlüssel
- Softwareupdates

Eine aktuelle Liste mit den Profilen finden Sie im Dokument „Configuration Profile Reference“ unter help.apple.com/deployment/mdm/#/mdm5370d089.

Konfigurationsprofile können signiert und verschlüsselt werden, um ihre Herkunft zu validieren, ihre Integrität zu gewährleisten und ihren Inhalt zu schützen. Außerdem können Konfigurationsprofile auf einem Mac gesperrt werden, um zu verhindern, dass sie gelöscht werden, oder um das Löschen erst nach Eingabe eines Passworts zuzulassen. Konfigurationsprofile, die einen Mac bei einer MDM-Lösung registrieren, können entfernt werden – dabei werden jedoch auch die verwalteten Konfigurationsinformationen, Daten und Apps gelöscht.

Benutzer können Konfigurationsprofile installieren, die in Safari geladen, per E-Mail versendet oder mit einer MDM-Lösung drahtlos übermittelt wurden. Wenn ein Benutzer einen Mac im DEP oder in Apple School Manager einrichtet, lädt und installiert der Computer automatisch ein Profil für die MDM-Registrierung.

MDM

Dank der MDM-Unterstützung in macOS können Unternehmen skalierte Mac, iPhone, iPad und Apple TV Implementierungen in ihrer gesamten Organisation sicher konfigurieren und verwalten. Die MDM-Funktionen basieren auf vorhandenen macOS Technologien wie Konfigurationsprofilen, der drahtlosen Registrierung und dem Apple Dienst für Push-Benachrichtigungen (Apple Push Notification service, APNs). So wird beispielsweise APNs verwendet, um den Ruhezustand eines Geräts zu beenden, damit es über eine sichere Verbindung direkt mit seinem MDM-Server kommunizieren kann. Über APNs werden keine vertraulichen oder unternehmensinternen Informationen übertragen.

Mit MDM können IT-Abteilungen den Mac in einer Unternehmensumgebung registrieren, drahtlos Einstellungen konfigurieren und aktualisieren, die Einhaltung von Unternehmensrichtlinien überwachen und verwaltete Mac Computer sogar per Fernzugriff löschen oder sperren.

Geräteregistrierung

Die Geräteregistrierung ist Teil von Apple School Manager und den Apple Bereitstellungsprogrammen. Sie bietet eine schnelle, optimierte Methode für die Implementierung von Mac Computern, die ein Unternehmen direkt bei Apple oder bei einem teilnehmenden autorisierten Apple Händler erworben hat.

Unternehmen können Computer automatisch bei MDM registrieren, ohne sie anzufassen oder vorzubereiten, bevor die Benutzer sie erhalten. Nach der Registrierung melden sich Administratoren auf der Website des Programms an und verknüpfen das Programm mit ihrer MDM-Lösung. Die von ihnen gekauften Computer können anschließend mit einer MDM-Lösung automatisch zugewiesen werden. Sobald ein Mac registriert wurde, werden in MDM festgelegte Konfigurationen, Einschränkungen und Steuerungen automatisch installiert. Die gesamte Kommunikation zwischen den Computern und den Apple-Servern wird mit HTTPS (SSL) verschlüsselt.

Die Einrichtung kann für die Benutzer noch weiter vereinfacht werden, indem bestimmte Schritte im Systemassistenten übersprungen werden, damit Benutzer schnell mit ihrer Arbeit beginnen können. Administratoren können außerdem steuern, ob der Benutzer das MDM-Profil vom Computer entfernen darf, und sicherstellen, dass Geräteeinschränkungen vom ersten Moment an greifen. Nach dem Auspacken und Aktivieren des Computers wird er bei der MDM-Lösung des Unternehmens registriert und alle verwalteten Einstellungen, Apps und Bücher werden installiert. Hinweis: Die Geräteregistrierung steht nicht in allen Ländern oder Regionen zur Verfügung.

Weitere Informationen für Unternehmen finden Sie in der Hilfe zu den Apple-Bereitstellungsprogrammen unter help.apple.com/deployment/business. Weitere Informationen für den Bildungsbereich finden Sie in der Hilfe zu Apple School Manager unter help.apple.com/schoolmanager.

Einschränkungen

Einschränkungen können von Administratoren aktiviert – oder in einigen Fällen deaktiviert – werden, um zu verhindern, dass Benutzer auf eine bestimmte App, einen bestimmten Dienst oder eine bestimmte Funktion des Geräts zugreifen können. Die Einschränkungen werden in einer Payload, die in einem Konfigurationsprofil enthalten ist, an die Geräte gesendet. Einschränkungen können auf macOS, iOS und tvOS Geräte angewendet werden.

Eine aktuelle Liste mit verfügbaren Einschränkungen für IT Manager finden Sie unter help.apple.com/deployment/mdm/#/mdm2pHf95672

Fernlöschen und Fernsperren

Mac Computer können von einem Administrator oder Benutzer per Fernzugriff gelöscht werden. Das sofortige Fernlöschen steht nur auf Macs zur Verfügung, auf denen FileVault aktiviert ist. Wenn MDM oder iCloud die Fernlöschung auslösen, sendet der Computer eine Bestätigung und führt den Löschvorgang durch. Beim Fernsperren erfordert MDM die Eingabe eines sechsstelligen Codes auf dem Mac. Benutzer können sich erst anmelden, wenn sie diesen Code eingegeben haben.

Datenschutz

Bei Apple sind wir überzeugt, dass Datenschutz ein grundlegendes Menschenrecht ist. Deshalb wird jedes Apple Produkt so entwickelt, dass es, wenn immer dies möglich ist, die geräteinterne Verarbeitung nutzt, die Erfassung und Verwendung von Daten begrenzt, Transparenz und Kontrolle über Ihre Informationen gewährleistet und eine starke Sicherheitsgrundlage bietet.

Apple hat zahlreiche Steuerungen und Optionen integriert, über die macOS Benutzer entscheiden können, wie und wann Apps ihre Daten nutzen und welche Daten verwendet werden. Weitere Informationen finden Sie unter www.apple.com/de/privacy.