Apple at Work

Plattformsicherheit

Von Grund auf sicher.

Bei Apple ist Sicherheit sehr wichtig – sowohl für die Benutzer:innen als auch zum Schutz von Unternehmensdaten. Deshalb integrieren wir von Anfang an fortschrittliche Sicherheitsfeatures in unsere Produkte, sodass sie von Grund auf sicher sind. Gleichzeitig achten wir darauf, ein tolles Benutzererlebnis zu gewährleisten, damit die Benutzer:innen so arbeiten können, wie sie es möchten. Nur Apple kann einen so umfassenden Schutz bieten, da wir Produkte mit integrierter Hardware, Software und Services entwickeln.

Hardwaresicherheit
Sichere Software erfordert eine Sicherheitsgrundlage, die in der Hardware integriert ist. Aus diesem Grund haben Apple Geräte, die unter iOS, iPadOS, macOS, tvOS oder watchOS laufen, Sicherheitsfeatures direkt in den Chips integriert.

Dazu gehören spezielle CPU Eigenschaften, die im System verankerte Sicherheitsfeatures ermöglichen, sowie zusätzliche Chips für reine Sicherheitsfunktionen. Die Hardware ist auf Sicherheit ausgerichtet und unterstützt prinzipiell nur eingeschränkte und eigenständige Funktionen, um möglichst wenig Angriffsfläche zu bieten. Zu solchen Komponenten gehören ein Boot-ROM, der als Hardware-Vertrauensanker für das sichere Booten fungiert, dedizierte AES Engines für effiziente und schnelle Ver- bzw. Entschlüsselung sowie eine Secure Enclave.

Die Secure Enclave ist ein System auf einem Chip (SoC) und befindet sich auf allen aktuellen iPhone, iPad, Apple Watch, Apple TV und HomePod Geräten sowie auf allen Mac Computern mit Apple Chip oder Apple T2 Security Chip. Sie folgt demselben Designprinzip wie das SoC und enthält jeweils einen eigenen, eigenständigen Boot-ROM und eine entsprechende AES Engine. Die Secure Enclave bietet zudem die Grundlage für das sichere Erstellen und Speichern von Schlüsseln, die zum Verschlüsseln von Daten im Speicher benötigt werden. Und sie schützt die biometrischen Daten für Touch ID und Face ID und wertet sie aus.

Speicherverschlüsselung muss schnell und effizient sein. Gleichzeitig aber dürfen Daten (oder Verschlüsselungsmaterial), die zum Erstellen der kryptographischen Schlüsselbeziehungen verwendet werden, nicht offengelegt werden. Die AES Hardware-Engine löst dieses Problem, indem sie eine schnelle integrierte Verschlüsselung und Entschlüsselung durchführt, während Dateien

geschrieben oder gelesen werden. Ein spezieller Kanal der Secure Enclave stellt der AES Engine das nötige Verschlüsselungsmaterial zur Verfügung, ohne die Informationen dabei für den Anwendungsprozessor (oder die CPU) oder das Betriebssystem selbst offenzulegen. So wird sichergestellt, dass die Apple Data Protection und FileVault Technologien die Dateien der Benutzer:innen schützen, ohne langfristig verwendete Verschlüsselungsschlüssel offenzulegen.

Apple hat den sicheren Bootprozess so entwickelt, dass die untersten Softwareebenen vor Manipulation geschützt sind und beim Starten nur vertrauenswürdige Betriebssystem-Software von Apple geladen wird. Der sichere Bootprozess startet mit dem unveränderlichen Code, dem sogenannten Boot-ROM, der bei der Herstellung des Apple SoC integriert wird und als Hardware-Vertrauensanker bekannt ist. Auf Mac Computern mit T2 Chip beginnt das Vertrauen in das sichere Booten von macOS mit dem T2. (Sowohl der T2 Chip als auch die Secure Enclave führen zudem ihren eigenen sicheren Bootprozess durch, jeweils mit eigenem, separatem Boot-ROM. Dies entspricht genau der Art und Weise, wie die Chips der A-Serie und im M1 sicher booten.)

Die Secure Enclave verarbeitet auch Fingerabdruck- und Gesichtsdaten der Touch ID und Face ID Sensoren in Apple Geräten. Dies ermöglichte eine sichere Authentifizierung, bei der die biometrischen Benutzerdaten privat und sicher bleiben. Außerdem profitieren Benutzer:innen so von der Sicherheit längerer und komplexer Codes und Passwörter und können sich in vielen Situationen schnell für Zugriff oder zum Bezahlen authentifizieren lassen.

Diese Sicherheitsfeatures in Apple Geräten werden durch die Kombination aus Chipdesign, Hardware, Software und Services ermöglicht, die es nur bei Apple gibt.

Systemsicherheit
Die Systemsicherheit baut auf den einzigartigen Möglichkeiten der Apple Hardware auf und steuert den Zugriff auf Systemressourcen in Apple Geräten, ohne die Benutzerfreundlichkeit zu beeinträchtigen. Die umfasst den Bootprozess, Softwareupdates und den Schutz von Computersystem-Ressourcen wie CPU, Arbeitsspeicher, Festplatte, Softwareprogramme und gesicherte Daten.

Die neuesten Versionen der Apple Betriebssysteme sind auch die sichersten. Ein wichtiger Teil der Apple Sicherheit ist das sichere Booten, das das System vor Malware-Angriffen während des Systemstarts schützt. Das sichere Booten beginnt in der Hardware und baut über die Software eine Vertrauenskette auf, bei der jeder Schritt sicherstellt, dass der nächste korrekt funktioniert, bevor die Kontrolle übergegeben wird. Dieses Sicherheitsmodell unterstützt nicht nur den standardmäßigen Startvorgang von Apple Geräten, sondern auch die verschiedenen Möglichkeiten zur Wiederherstellung und zeitnahen Aktualisierung von Apple Geräten. Subkomponenten wie der T2 Chip und die Secure Enclave führen zudem ihren eigenen sicheren Bootprozess durch, um sicherzustellen, dass sie nur bekanntem Code von Apple booten. Das Updatesystem kann sogar sogenannte Downgradeangriffe verhindern, sodass die Geräte nicht auf ältere Versionen des Betriebssystems zurückgesetzt werden können (bei denen Angreifer wissen, wie sie sich Zugriff verschaffen), um Benutzerdaten zu stehlen.

Apple Geräte verfügen zudem über einen Boot- und Laufzeitschutz, sodass sie auch in Betrieb sicher bleiben. Von Apple entwickelte Chips in iPhone, iPad, Apple Watch, Apple TV und HomePod sowie Apple Chips in Mac Computern

haben eine einheitliche Architektur, um die Integrität des Betriebssystems zu schützen. macOS bietet zudem eine erweiterte und konfigurierbare Auswahl an Schutzmöglichkeiten für sein abweichendes Computingmodell sowie mit Features, die auf allen Mac Hardware-Plattformen unterstützt werden.

Verschlüsselung und Datenschutz
Apple Geräte verfügen über Verschlüsselungsfeatures, um die Benutzerdaten zu schützen und eine Fernlöschung zu ermöglichen, falls ein Gerät gestohlen wird oder verloren geht.

Die Funktionen für eine sichere Bootkette, System-Sicherheit und App-Sicherheit helfen dabei, dass nur Code und Apps auf dem Gerät ausgeführt werden, die vertrauenswürdig sind. Apple Geräte haben zusätzliche Verschlüsselungsfeatures, um die Benutzerdaten zu schützen, selbst wenn andere Teile der Sicherheitsinfrastruktur kompromittiert wurden – beispielsweise wenn ein Gerät verloren ging oder nicht vertrauenswürdiger Code verwendet wird. Von all diesen Features profitieren nicht nur Benutzer:innen, sondern auch für IT-Admins. Sie schützen persönliche und unternehmenseigene Daten und erlauben eine sofortige und vollständige Fernlöschung auf gestohlenen oder verlorenen Geräten.

iOS und iPadOS Geräte verwenden eine Dateiverschlüsselungsmethode namens Data Protection, während Daten auf einem Mac mit Intel Prozessor mit einer Laufwerksverschlüsselung namens FileVault geschützt werden. Mac Computer mit Apple Chip verwenden ein Hybridmodell, das Data Protection unterstützt und zwei Sicherheitsmaßnahmen umfasst: Die niedrigste Schutzklasse (Class D) wird nicht unterstützt und die Standardklasse (Class C) verwendet einen Laufwerksschlüssel und verhält sich genau wie FileVault auf einem Mac mit Intel Prozessor. In allen Fällen befinden sich die Hierarchien für die Schlüsselverwaltung im dedizierten Chip der Secure Enclave und eine dedizierte AES Engine unterstützt die Verschlüsselung in Leitungsgeschwindigkeit und sorgt dafür, dass langfristig verwendete Schlüssel nicht in das Kernel-Betriebssystem oder die CPU gelangen, wo sie kompromittiert werden könnten. (Ein Mac mit Intel Prozessor und T1 Chip oder ohne Secure Enclave verwendet keinen dedizierten Chip, um seine FileVault Verschlüsselungsschlüssel zu schützen.)

Ergänzend zum Schutz vor unerlaubtem Datenzugriff, den Data Protection und FileVault bieten, setzen die Apple Betriebssystemkernel Schutz- und Sicherheitsmaßnahmen durch. Der Kernel nutzt Zugriffskontrollen, um Apps in Sandboxes auszuführen und so zu beschränken, auf welche Daten Apps zugreifen können. Außerdem kommt ein Mechanismus namens Data Vault zum Einsatz. Dieser beschränkt den Zugriff auf die Daten einer App durch alle anderen Apps, die eine entsprechende Anfrage stellen, statt die Aufrufe durch eine App zu beschränken.

Sicherheit von Apps
Apps gehören zu den kritischsten Elementen einer Sicherheitsarchitektur. Auch wenn Apps den Benutzer:innen unglaubliche Produktivitätsvorteile bringen, können sie auch die Systemsicherheit, Stabilität und Benutzerdaten beeinträchtigen, falls sie nicht angemessen gehandhabt werden.

Daher bietet Apple mehrere Schutzebenen, um sicherzustellen, dass Apps keine bekannte Malware enthalten und nicht manipuliert wurden. Weitere

Schutzmaßnahmen erzwingen, dass der Zugriff von Apps auf Benutzerdaten sorgfältig gehandhabt wird. Diese Sicherheitsprotokolle bieten eine stabile, sichere Plattform für Apps und ermöglichen es Tausenden von Entwickler:innen, Hunderttausende von Apps für iOS, iPadOS und macOS bereitzustellen – alles ohne die Systemintegrität zu gefährden. Und Benutzer:innen können auf ihren Apple Geräten auf diese Apps zugreifen, ohne sich unnötig Sorgen wegen Viren, Malware oder unbefugten Angriffen zu machen.

Auf iPhone, iPad und iPod touch kommen alle Apps aus dem App Store und laufen in Sandboxes, um einen optimalen Schutz zu gewährleisten.

Auf dem Mac kommen zwar viele Apps aus dem App Store, aber Mac Benutzer:innen laden und verwenden auch Apps aus dem Internet. Für sichere Downloads aus dem Internet hat macOS zusätzliche Schutzmaßnahmen integriert. Zunächst müssen ab macOS 10.15 standardmäßig alle Mac Apps vor dem Öffnen von Apple genehmigt werden. Diese Voraussetzung hilft sicherzustellen, dass die Apps frei von bekannter Malware sind, ohne dass die Apps aus dem App Store stammen müssten. Zudem bietet macOS modernsten Antivirenschutz, um Malware zu blockieren und bei Bedarf zu entfernen.

Als zusätzliche Kontrolle über die Plattformen hinweg hilft Sandboxing dabei, Benutzerdaten vor unbefugtem Zugriff durch Apps zu schützen. Und in macOS werden Daten in kritischen Bereichen direkt geschützt. Das stellt sicher, dass Benutzer:innen die Kontrolle über den Zugriff durch alle Apps auf Dateien in „Schreibtisch", „Dokumente", „Downloads" und anderen Bereichen behalten – egal ob die zugreifenden Apps selbst in einer Sandbox laufen oder nicht.

Sicherheit von Services
Apple hat robuste Services entwickelt, mit denen die Benutzer:innen noch mehr mit ihren Geräten machen und noch produktiver sein können. Diese Dienste bieten leistungsstarke Möglichkeiten für Cloudspeicherung, Synchronisierung, Passwortsicherung, Authentifizierung, Bezahlvorgänge, Nachrichten, Kommunikation und mehr – während gleichzeitig die Privatsphäre der Benutzer:innen und die Sicherheit ihrer Daten geschützt bleiben.

Zu diesen Services gehören iCloud, Mit Apple anmelden, Apple Pay, iMessage, Business Chat, FaceTime, Wo ist? und Integration – möglicherweise erfordern sie eine Apple ID oder verwaltete Apple ID. In einigen Fällen kann eine verwaltete Apple ID nicht mit einem bestimmten Apple Service verwendet werden, beispielsweise bei Apple Pay.

Hinweis: Nicht alle Apple Services und Inhalte sind in allen Ländern oder Regionen verfügbar.

Netzwerksicherheit – Übersicht
Zusätzlich zu den integrierten Sicherheitsfeatures, die Apple zum Schutz der auf Apple Geräten gespeicherten Daten verwendet, gibt es viele Maßnahmen, mit denen Unternehmen ihre Daten bei der Übertragung von Gerät zu Gerät schützen können. Alle diese Sicherheitsfeatures und Maßnahmen fallen unter die Netzwerksicherheit.

Benutzer:innen müssen von überall auf der Welt auf Unternehmensnetzwerke zugreifen können. Daher muss sichergestellt werden, dass sie autorisiert sind und ihre Daten während der Übertragung geschützt bleiben. Um diese

Sicherheitsziele zu erreichen, integrieren iOS, iPadOS und macOS bewährte Technologien und die aktuellsten Standards für Netzwerkverbindungen über WLAN und mobile Daten. Das ist auch der Grund, warum unsere Betriebssysteme standardmäßige Netzwerkprotokolle für authentifizierte, autorisierte und verschlüsselte Kommunikation verwenden – und Entwickler:innen Zugriff darauf bieten.

Weitere Infos zur Sicherheit mit Apple Geräten.

apple.com/de/business/it

apple.com/de/macos/security

apple.com/de/privacy/features

apple.com/security

Partner-Ökosystem

Apple Geräte sind mit häufig in Unternehmen verwendeten Sicherheitstools und -services kompatibel, um sicherzustellen, dass die Geräte und die darauf gespeicherten Daten allen Vorgaben entsprechen. Jede Plattform unterstützt Standardprotokolle für VPN – auch VPN-Verbindungen pro Account unter iOS und iPadOS 14 – sowie sicheres WLAN zum Schutz von Netzwerktraffic und stellt sichere Verbindungen zu üblichen Unternehmensinfrastrukturen her.

Die Partnerschaft von Apple mit Cisco ermöglicht verbesserte Sicherheit und Produktivität, wenn die Produkte und Services beider Unternehmen kombiniert werden. Cisco Netzwerke bieten verbesserte Sicherheit über den Cisco Security Connector und gewähren Business-Anwendungen Vorrang in Cisco Netzwerken.