Apple at Work

Plattformsicherheit

Sicherheit ist eingebaut.

Bei Apple ist Sicherheit sehr wichtig – sowohl für die Benutzer:innen als auch zum Schutz von Unternehmensdaten. Von Anfang an sind fortschrittliche Sicherheitsfeatures in die Produkte integriert – sodass sie von Grund auf sicher sind. Gleichzeitig sorgt Apple für ein großartiges Benutzererlebnis, damit alle so arbeiten können, wie sie möchten. Nur Apple kann einen so umfassenden Schutz bieten, weil die Produkte mit integrierter Hardware, Software und Services entwickelt werden.

Hardwaresicherheit
Sichere Software erfordert eine Sicherheitsgrundlage, die in der Hardware integriert ist. Darum haben Apple Geräte, die mit iOS, iPadOS, macOS, tvOS oder watchOS laufen, Funktionen für Sicherheit 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 diesen Hardwarekomponenten gehören ein Boot ROM, der einen Hardware-Vertrauensanker (Root of Trust) für sichere Bootfunktionen bildet, dedizierte AES Engines für eine effiziente und sichere Verschlüsselung und Entschlüsselung sowie eine Secure Enclave.

Die Secure Enclave ist ein System auf dem Chip (SoC) und befindet sich auf allen iPhone, iPad, Apple Watch, Apple TV und HomePod Geräten der aktuellen Generation 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 bildet außerdem die Grundlage für die sichere Erstellung und Speicherung der Codes, die zur Verschlüsselung von Daten im Ruhezustand benötigt werden. Und sie schützt die biometrischen Daten für Touch ID und Face ID und wertet sie aus.

Speicherverschlüsselung muss schnell und effizient sein. Dabei darf sie die von ihr verwendeten Daten (oder das Schlüsselmaterial) aber nicht offenlegen, um kryptografische Schlüsselbeziehungen zu erstellen. Die AES Hardware Engine löst

dieses Problem, indem sie eine schnelle Inline Verschlüsselung und Entschlüsselung durchführt, während Dateien geschrieben oder gelesen werden. Ein spezieller Kanal der Secure Enclave stellt der AES Engine das nötige Schlüsselmaterial zur Verfügung, ohne diese Daten mit dem Anwendungsprozessor (oder CPU) oder dem allgemeinen Betriebssystem zu teilen. Dadurch wird sichergestellt, dass die Apple Data Protection und FileVault Technologien die Dateien von Benutzer:innen schützen, ohne langfristig verwendete Verschlüsselungscodes 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 namens 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 außerdem ihre eigenen sicheren Bootprozesse durch, jeweils mit eigenem, separatem Boot ROM. Dies läuft exakt identisch zum sicheren Booten in Chips der A-Serie und im M1.)

Die Secure Enclave verarbeitet auch Fingerabdruck- und Gesichtsdaten der Touch ID und Face ID Sensoren in Apple Geräten. Das ermöglicht eine sichere Authentifizierung und sorgt dafür, dass biometrische Nutzerdaten privat und sicher bleiben. Außerdem profitieren so alle 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 Systemsicherheit umfasst den Bootprozess, Softwareupdates und den Schutz von Computer-Systemressourcen 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. Es schützt das System vor Malware-Angriffen während des Systemstarts. Das sichere Booten beginnt in der Hardware und baut über die Software eine Vertrauenskette auf. Dabei sorgt jeder Schritt dafür, dass der nächste korrekt funktioniert, bevor die Kontrolle übergeben wird. Dieses Sicherheitsmodell unterstützt nicht nur den Standardprozess beim Starten von Apple Geräten, sondern auch diverse Möglichkeiten zur Wiederherstellung und zeitnahen Aktualisierung von Apple Services. Subkomponenten wie der T2 Chip und die Secure Enclave führen außerdem ihren eigenen sicheren Bootprozess durch, um sicherzustellen, dass sie nur bekannten Code von Apple booten. Das Updatesystem kann sogar Downgradeangriffe verhindern. So können keine älteren Betriebssystemversionen (bei denen Angreifer wissen, wie sie sich Zugriff verschaffen) installiert werden, um Daten zu stehlen.

Apple Geräte enthalten außerdem einen Boot- und Laufzeitschutz, damit sie auch sicher sind, während sie arbeiten. Von Apple entwickelte Chips in iPhone, iPad, Apple Watch, Apple TV und HomePod und Apple Chips in Mac Computern haben eine einheitliche Architektur zum Schutz der Betriebssystem-Integrität. macOS kommt außerdem mit erweiterten, einstellbaren Schutzmöglichkeiten für sein abweichendes Computingmodell sowie mit Features, die auf allen Mac Hardware-Plattformen unterstützt werden.

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

Die Funktionen für eine sichere Bootkette, Systemsicherheit und App Sicherheit helfen dabei, dass nur Code und Apps auf dem Gerät ausgeführt werden, die vertrauenswürdig sind. Apple Geräte haben zusätzliche Verschlüsselungsfeatures, die Benutzerdaten auch dann schützen, wenn andere Teile der Sicherheitsinfrastruktur kompromittiert wurden. Zum Beispiel wenn ein Gerät verloren gegangen ist oder nicht vertrauenswürdiger Code darauf ausgeführt wird. Alle diese Features haben nicht nur Vorteile für 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 nutzen eine Methode zur Verschlüsselung von Dateien, die Data Protection heißt. Die Daten auf Mac Computern mit Intel Prozessoren werden mit einer Laufwerksverschlüsselung namens FileVault geschützt. Mac Computer mit Apple Chip nutzen ein Hybridmodell, das Data Protection unterstützt und zwei Sicherheitsmaßnahmen umfasst: Die niedrigste Schutzklasse (Class D) wird nicht unterstützt und das Standardlevel (Class C) nutzt einen Laufwerkschlüssel 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 Verschlüsselungscodes 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 nutzt keinen dedizierten Chip, um seine FileVault Verschlüsselungscodes zu schützen.)

Neben dem Einsatz der Data Protection und FileVault Features, die unbefugte Zugriffe auf Daten verhindern, setzen Apple Betriebssystem-Kernel Schutz und Sicherheit 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.

App Sicherheit
Apps gehören zu den kritischsten Elementen einer Sicherheitsarchitektur. Obwohl Apps unglaubliche Vorteile bei der Produktivität bringen, können sie auch die Systemsicherheit, Stabilität und Benutzerdaten beeinträchtigen, falls sie nicht angemessen gehandhabt werden.

Darum nutzt Apple mehrere Schutzebenen, um sicherzustellen, dass Apps keine Malware enthalten und nicht manipuliert wurden. Zusätzliche Schutzmaßnahmen stellen eine sichere Übertragung von Benutzerdaten an Apps sicher. Diese Sicherheitsprotokolle sorgen für eine stabile, sichere Plattform für Apps und ermöglichen es Tausenden von Entwickler:innen, Hunderttausende von Apps für iOS, iPadOS und macOS bereitzustellen – ohne die Systemintegrität zu gefährden. Und dass alle mit ihren Apple Geräten auf alle diese Apps zugreifen können, 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 optimale Sicherheit zu gewährleisten.

Auf dem Mac kommen zwar viele Apps aus dem App Store, aber Mac Benutzer:innen laden und nutzen auch Apps aus dem Internet. Für sichere Downloads aus dem Internet hat macOS zusätzliche Schutzmaßnahmen integriert. Zunächst einmal müssen ab macOS 10.15 alle Mac Apps vor dem Öffnen von Apple genehmigt werden. Das soll verhindern, dass diese Apps Malware enthalten, ohne dass sie aus dem App Store stammen müssen. Zusätzlich bietet macOS modernsten Antivirenschutz, um Malware zu blockieren und, wenn nötig, zu entfernen.

Als zusätzliche plattformübergreifende Kontrolle 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 – unabhängig davon, ob die zugreifenden Apps selbst in einer Sandbox sind oder nicht.

Sicherheit von Services
Apple hat eine Reihe robuster Services entwickelt, mit denen alle noch mehr mit ihren Geräten machen und noch produktiver sein können. Diese Services bieten leistungsstarke Möglichkeiten zum Speichern in der Cloud, Synchronisieren, Sichern von Passwörtern, Authentifizieren, Bezahlen, Versenden von Nachrichten, Austauschen von Kommunikation und mehr – gleichzeitig bleiben Privatsphäre und Daten geschützt.

Zu diesen Services zählen iCloud, Mit Apple anmelden, Apple Pay, iMessage, Business Chat, FaceTime, Wo ist? und Integration. Eventuell ist eine Apple ID oder verwaltete Apple ID erforderlich, um sie zu nutzen. In einigen Fällen kann eine verwaltete Apple ID nicht mit einem bestimmten Service verwendet werden, etwa bei Apple Pay.

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

Netzwerksicherheit – Übersicht
Apple setzt nicht nur auf integrierte Sicherheitsfeatures zum Schutz von Daten, die auf Apple Geräten gespeichert sind. Es gibt viele weitere 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. Darum ist es wichtig, dass sie autorisiert sind und dass ihre Daten bei der Übertragung geschützt bleiben. Um diese Sicherheitsziele zu erreichen, integrieren iOS, iPadOS und macOS bewährte Technologien und die neuesten Standards für Netzwerkverbindungen über WLAN und mobile Daten. Das ist auch der Grund, warum die Betriebssysteme von Apple standardmäßige Netzwerkprotokolle für eine authentifizierte, autorisierte und verschlüsselte Kommunikation verwenden – und Entwicklern Zugriff darauf geben.

Partner-Ökosystem

Apple Geräte sind mit häufig in Unternehmen verwendeten Sicherheitstools und -services kompatibel. Dadurch entsprechen die Geräte und die darauf gespeicherten Daten immer den geltenden Vorgaben. Jede Plattform unterstützt Standardprotokolle für VPN – inklusive VPN Verbindungen pro Account auf iOS 14 und iPadOS 14 – und sicheres WLAN zum Schutz von Netzwerktraffic und stellt sichere Verbindungen zu üblichen Unternehmensinfrastrukturen her.

Die Zusammenarbeit von Apple und Cisco sorgt für verbesserte Sicherheit und Produktivität, wenn die Produkte und Services beider Unternehmen kombiniert werden. Cisco Netzwerke bieten verbesserte Sicherheit durch den Cisco Security Connector und geben Business-Anwendungen in Cisco Netzwerken Priorität.

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