Apple at Work

Plattformsicherheit

Von Grund auf sicher.

Bei Apple nehmen wir Sicherheit sehr ernst, sowohl für die Nutzer als auch beim Schutz von Unternehmensdaten. Deshalb integrieren wir von Anfang an modernste Sicherheitslösungen in unsere Produkte, sodass sie von Grund auf sicher sind. Gleichzeitig achten wir darauf, ein fantastisches Benutzererlebnis zu gewährleisten, damit die Benutzer so arbeiten können, wie sie es möchten. Dieses umfassende Sicherheitskonzept kann nur Apple bieten, da wir Produkte mit integrierter Hardware, Software und Services entwickeln.

Hardware-Sicherheit
Sichere Software braucht eine sichere Basis, die bereits in die Hardware integriert ist. Aus diesem Grund haben Apple Geräte, die unter iOS, iPadOS, macOS, tvOS oder watchOS laufen, Sicherheitsfeatures, die auf der Ebene der Chips angesiedelt sind.

Dazu gehören speziell entwickelte Fähigkeiten der CPU, die Sicherheitsfeatures des Systems unterstützen, und Chips, die Sicherheitsfunktionen gewidmet sind. Die wichtigste Komponente ist der Secure Enclave Coprozessor in modernen iOS, iPadOS, watchOS und tvOS Geräten sowie in allen Mac Computern mit Apple T2 Security Chip. Secure Enclave bietet die Grundlage für die Verschlüsselung unbenutzter Daten, sicheres Starten in macOS und die Verwendung biometrischer Daten.

Alle modernen iPhone, iPad und Mac mit T2 Chip verfügen über eine AES Hardware-Engine für Line-Speed-Verschlüsselung beim Lesen und Schreiben von Dateien. So können Data Protection und FileVault die Benutzerdaten schützen, ohne dass langlebige Schlüssel für die CPU oder das Betriebssystem offen liegen.

Der sichere Start von Apple Geräten bedeutet, dass die unterste Software-Ebene nicht beeinflusst wird und beim Systemstart nur vertrauenswürdige Systemsoftware von Apple geladen wird. Bei iOS und iPadOS Geräten beginnt Sicherheit mit dem unveränderlichen Code, dem sogenannten Boot ROM. Dieser wird bei der Chipherstellung festgelegt und ist auch als Hardware-Vertrauensanker bekannt. Auf Mac Computern mit T2 Chip wird Vertrauen für den sicheren Systemstart direkt in der Secure Enclave erzeugt.

Die Secure Enclave ermöglicht es Touch ID und Face ID in Apple Geräten, sichere Authentifizierungen durchzuführen und gleichzeitig die biometrischen Daten der Benutzer sicher und vertraulich zu halten. So können Nutzer längere und komplexere Codes und Passwörter verwenden und sich in vielen Situationen dennoch schnell und einfach anmelden.

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

Systemsicherheit
Auf Basis der einzigartigen Fähigkeiten von Apple Hardware ist die Systemsicherheit darauf ausgelegt, die Sicherheit des Betriebssystems auf Apple Geräten zu maximieren, ohne dabei das Benutzererlebnis zu beeinträchtigen. Die Systemsicherheit umfasst dabei den Systemstart, Software-Updates und die anhaltende Verwendung des Betriebssystems.

Der sichere Systemstart beginnt bei der Hardware und folgt einer Vertrauenskette mit Software, bei der jeder Schritt sicherstellt, dass der nächste korrekt funktioniert, bevor die Kontrolle abgegeben wird. Dieses Sicherheitsmodell unterstützt nicht nur den standardmässigen Startvorgang von Apple Geräten, sondern auch die verschiedenen Modi für Wiederherstellung und Aktualisierung von iOS, iPadOS und macOS Geräten.

Die aktuellsten Versionen von iOS, iPadOS und macOS sind die sichersten. Der Mechanismus für Softwareaktualisierungen bietet nicht nur zeitnahe Updates für Apple Geräte – er bietet auch ausschliesslich vertrauenswürdige Software von Apple. Das Aktualisierungssystem verhindert sogar sogenannte Downgrade-Angriffe, sodass die Geräte nicht auf eine vorherige Version des Betriebssystems zurückgesetzt werden können, um Benutzerdaten zu stehlen.

Zudem verfügen Apple Geräte über Schutz beim Systemstart und über Laufzeitschutz, sodass sie auch in Betrieb sicher bleiben. Diese Schutzarten funktionieren auf iOS, iPadOS und macOS sehr unterschiedlich – je nach den unterschiedlichen Fähigkeiten, die sie haben, und den unterschiedlichen Angriffen, gegen die sie sich dadurch wehren müssen.

Um dieses hohe Mass an Schutz zu erreichen, verwenden iOS und iPadOS Kernel Integrity Protection, System Coprocessor Integrity, Pointer Authentication Codes und Page Protection Layer. macOS hingegen setzt auf Unified Extensible Firmware Interface Security, System Management Mode, Direct Memory Access Protections und Peripheral Firmware Security.

Verschlüsselung und Datenschutz
Apple Geräte verfügen über Verschlüsselungsfeatures, um die Benutzerdaten zu schützen und im Falle von Diebstahl oder Verlust das Löschen aus der Entfernung zu ermöglichen.

Die sichere Bootkette, Systemsicherheit und die Sicherheitsfeatures für Apps tragen dazu bei, dass nur vertrauenswürdige Codes und Apps auf einem Gerät ausgeführt werden können. Apple Geräte haben zusätzliche Verschlüsselungsfeatures, um die Benutzerdaten zu schützen, selbst wenn andere Teile der Sicherheitsinfrastruktur kompromittiert wurden – beispielsweise, wenn ein Gerät verloren wurde oder Code verwendet wird, der nicht

vertrauenswürdig ist. Von all diesen Features profitieren die Benutzer und IT-Administratoren. Dabei werden sowohl persönliche als auch Unternehmensdaten immer geschützt und Möglichkeiten geboten, im Falle von Diebstahl oder Verlust alle Daten aus der Entfernung zu löschen.

iOS und iPadOS Geräte verwenden eine Dateiverschlüsselungsmethode namens Data Protection, während Daten auf dem Mac mit einer Laufwerksverschlüsselung namens FileVault geschützt werden. Beide Vorgehensweisen verankern ihre Hierarchie für die Verwaltung von Schlüsseln auf Geräten, die über einen SEP verfügen, im dedizierten Sicherheitschip der Secure Enclave. Beide Vorgehensweisen nutzen ausserdem die dedizierte AES Engine, um Line-Speed-Verschlüsselung zu unterstützen und sicherzustellen, dass langlebige Schlüssel nie an den Kernel des Betriebssystems oder die CPU weitergegeben werden, wo sie gegebenenfalls kompromittiert werden könnten.

Sicherheit von Apps

Apps gehören zu den kritischsten Elementen einer modernen Sicherheitsarchitektur. Während Apps den Benutzern fantastische Produktivitätsvorteile bieten, können sie auch potenziell negative Auswirkungen auf die Sicherheit des Systems und der Benutzerdaten haben, wenn sie nicht richtig gehandhabt werden. Apple bietet mehrere Sicherheitsebenen, um sicherzustellen, dass Apps keine bekannten Schadprogramme enthalten und nicht manipuliert wurden. Für den Zugriff auf Benutzerdaten durch Apps werden weitere Sicherheitsmassnahmen erzwungen und der Vorgang wird sorgfältig verwaltet.

Integrierte Sicherheitskontrollen bieten eine stabile, sichere Plattform für Apps und ermöglichen es Tausenden von Entwicklern, Hunderttausende von Apps zur Verfügung zu stellen – alles ohne die Integrität des Systems zu beeinträchtigen. Und die Benutzer können diese Apps auf ihren Geräten verwenden, wo Kontrollen durchgeführt werden, die vor Viren, Schadsoftware und nicht-autorisierten Angriffen schützen.

Auf iPhone, iPad und iPod touch kommen alle Apps aus dem App Store – und alle Apps laufen in einer Sandbox, um die bestmögliche Kontrolle zu bieten. Auf dem Mac kommen viele Apps aus dem App Store, aber Mac Benutzer laden und verwenden auch Apps aus dem Internet. Um Downloads aus dem Internet sicher zu unterstützen, verwendet macOS zusätzliche Kontrollebenen. Zunächst müssen ab macOS 10.15 standardmässig alle Mac Apps von Apple notarisiert sein, um zu starten. Diese Voraussetzung stellt sicher, dass die Apps frei von bekannter Schadsoftware sind, ohne dass die Apps durch den App Store verteilt werden müssten. Zudem enthält macOS auch Antivirenschutz, der den Branchenstandards entspricht und bei Bedarf Schadsoftware blockiert oder entfernt.

Als zusätzliche Kontrolle über die Plattformen hinweg hilft Sandboxing dabei, die Benutzerdaten vor unberechtigtem Zugriff durch Apps zu schützen. Und in macOS werden Daten in kritischen Bereichen selbst in einer Sandbox verwahrt – was sicherstellt, dass die Benutzer die Kontrolle über den Dateizugriff in Schreibtisch, Dokumente, Downloads oder in anderen Bereichen behalten. Das gilt für alle Apps, egal ob die App, die den Zugriff versucht, selbst in einer Sandbox läuft oder nicht.

Sicherheit für Services

Apple hat robuste Services entwickelt, mit denen die Benutzer ihre Geräte noch besser und produktiver nutzen können. Zu diesen gehören Apple ID, iCloud, Mit Apple anmelden, Apple Pay, iMessage, FaceTime, Siri und Wo ist?. Diese Dienste bieten leistungsfähige Features für Cloudspeicherplatz und Synchronisation, Authentifizierung, Bezahlvorgänge, Nachrichten, Kommunikation und mehr – während gleichzeitig die Privatsphäre der Benutzer und die Sicherheit ihrer Daten geschützt werden.

Partner-Ökosystem

Apple Geräte arbeiten mit in Unternehmen häufig verwendeten Sicherheitstools und -diensten zusammen, um sicherzustellen, dass die Geräte und die darauf vorhandenen Daten alle Richtlinien einhalten. Jede Plattform unterstützt Standardprotokolle für VPN und sicheres WLAN, um Netzwerkverkehr zu schützen und sich sicher mit verbreiteter Unternehmensinfrastruktur zu verbinden.

Die Partnerschaft von Apple mit Cisco ermöglicht verbesserte Sicherheit und Produktivität. Cisco Netzwerke bieten verbesserte Sicherheit über den Cisco Security Connector und gewähren Anwendungen von Unternehmen Vorrang in Cisco Netzwerken.

Mehr zum Thema Sicherheit mit Apple Geräten.

apple.com/chde/business/it

apple.com/de/macos/security

apple.com/chde/privacy/features

apple.com/chde/security