Apple at Work

Platformbeveiliging

Veilig op alle fronten.

Beveiliging is voor Apple een belangrijk onderwerp. Niet alleen je gebruikers, ook je bedrijfsgegevens moeten goed worden beschermd. Door de geavanceerde ingebouwde beveiliging zijn onze producten op alle fronten veilig. En we hebben ervoor gezorgd dat de beveiliging het gebruiksgemak niet in de weg staat, zodat je werknemers kunnen werken zoals ze willen. Alleen Apple kan beveiliging op zo'n doortimmerde manier aanpakken – omdat we producten maken met geïntegreerde hardware, software en diensten.

Hardwarebeveiliging
Software kan alleen optimaal worden beveiligd als de basis daarvoor is ingebouwd in de software. Daarom zijn beveiligingsfeatures ingebouwd in alle Apple devices, of ze nu werken met iOS, iPadOS, macOS, tvOS of watchOS.

Hiertoe behoren speciale CPU-features die de basis vormen voor de systeembeveiliging en beveiligingsfeatures van de hardware. Het belangrijkste onderdeel is de Secure Enclave-coprocessor, die te vinden is in alle moderne iOS-, iPadOS-, watchOS- en tvOS-devices en alle Macs met Apple T2 Security-chip. De Secure Enclave vormt de basis voor de beveiliging van opgeslagen gegevens, de veilige opstartprocedure van macOS en de opslag van biometrische gegevens.

Alle moderne iPhones en iPads en alle Macs met T2-chip bevatten een speciale AES-hardware-engine voor de snelle versleuteling van bestanden die worden gelezen of weggeschreven. Zo kunnen gegevensbescherming en FileVault-versleuteling worden ingezet om bestanden te beveiligen, zonder dat langdurige coderingssleutels worden doorgegeven aan de CPU of het besturingssysteem.

De veilige opstartprocedure van Apple devices garandeert dat er niet is geknoeid op de laagste softwareniveaus en dat alleen vertrouwde OS-software van Apple wordt geladen bij het opstarten. De beveiliging van iOS- en iPadOS-devices begint met de onbewerkbare code van het Boot-ROM. Deze code, de 'Root of Trust' voor de hardware, wordt vastgelegd bij de fabricage van de chip. Op Macs met T2-chip is de Secure Enclave de vertrouwensbasis voor de veilige opstartprocedure.

De Secure Enclave zorgt dat gebruikers zich op Apple devices veilig kunnen aanmelden via Touch ID en Face ID zonder dat de biometrische gegevens van de gebruiker kunnen worden achterhaald. Zo profiteren gebruikers van een beveiliging op basis van langere, complexere toegangscodes en wachtwoorden en kunnen ze zich in de meeste gevallen toch snel aanmelden.

De beveiligingsfeatures van Apple devices worden mogelijk gemaakt door een combinatie van design, hardware, software en services die alleen Apple aanbiedt.

Systeembeveiliging
De systeembeveiliging, die is gebaseerd op unieke mogelijkheden van de Apple hardware, optimaliseert de beveiliging van het besturingssysteem zonder nadelige gevolgen voor het gebruiksgemak. De systeembeveiliging omvat de opstartprocedure, de installatie van software-updates en het continue gebruik van het besturingssysteem.

De veilige opstartprocedure begint bij de hardware en creëert een vertrouwensketen binnen de software, waarbij steeds wordt gecontroleerd of de volgende stap goed functioneert voordat de besturing wordt overgedragen. Dit beveiligingsmodel wordt niet alleen gebruikt bij de normale opstartprocedure van Apple devices, maar ook bij de verschillende procedures voor het herstellen en updaten van iOS-, iPadOS en macOS-devices.

De nieuwste versies van iOS, iPadOS en macOS bieden altijd de beste beveiliging. Met de procedure voor software-updates worden Apple devices niet alleen regelmatig bijgewerkt, maar kan ook alleen vertrouwde Apple software worden geïnstalleerd. Het updatesysteem kan zelfs downgrade-aanvallen voorkomen, zodat op devices geen eerdere versie van het besturingssysteem kan worden geïnstalleerd om gebruikersgegevens te stelen.

Ten slotte bieden Apple devices ook opstart- en runtimebeveiliging voor bescherming van de systeemintegriteit tijdens het gebruik. Voor de verschillende besturingssystemen (iOS, iPadOS en macOS) worden verschillende methoden gebruikt, omdat de features en dus ook de mogelijke aanvallen per device sterk verschillen.

In iOS en iPadOS is deze beveiliging gebaseerd op KIP (Kernel Integrity Protection), SCIP (System Coprocessor Integrity), PAC's (Pointer Authentication Codes) en PPL (Page Protection Layer), terwijl in macOS gebruik wordt gemaakt van UEFI-beveiliging (Unified Extensible Firmware Interface), SMM (System Management Mode), DMA-beveiliging (Direct Memory Access) en beveiliging van de firmware van randapparatuur.

Versleuteling en beveiliging van gegevens
Apple devices zijn uitgerust met versleutelingsfeatures om gebruikersgegevens te beschermen en devices op afstand te wissen bij diefstal of verlies.

Dankzij de beveiligde opstartsequentie en features voor systeem- en appbeveiliging kunnen alleen vertrouwde code en apps worden gebruikt op een device. Daarnaast zijn Apple devices uitgerust met extra versleutelingsfeatures om gebruikersgegevens te beschermen, zelfs als bepaalde onderdelen van de beveiligingsinfrastructuur niet langer veilig zijn – bijvoorbeeld bij verlies van het device of wanneer er niet-vertrouwde code wordt uitgevoerd. Al deze features bieden voordelen voor gebruikers en IT-beheerders. Persoonlijke en zakelijke gegevens zijn altijd beveiligd en bij verlies of diefstal kun je een device op afstand volledig wissen.

iOS- en iPadOS-devices werken op basis van Data Protection, een speciale versleutelingsmethode voor bestanden. De gegevens op Macs worden beveiligd met de FileVault-technologie voor volumeversleuteling. Bij beide methoden is de hiërarchie voor sleutelbeheer gebaseerd op de Secure Enclave van devices met een SEP. Beide methoden werken ook met een speciale AES-engine om elke regel te versleutelen en te voorkomen dat langdurige coderingssleutels worden doorgegeven aan het kernelbesturingssysteem of de CPU, omdat ze dan in verkeerde handen terecht zouden kunnen komen.

Beveiliging van apps

Apps vormen een van de belangrijkste factoren van een moderne beveiligingsarchitectuur. Hoewel apps de productiviteit van gebruikers enorm kunnen verhogen, kunnen ze bij verkeerd gebruik gevaren opleveren voor de beveiliging en stabiliteit van het systeem en de beveiliging van gebruikersgegevens. Apple heeft beveiligingslagen geïmplementeerd om te controleren of apps geen bekende malware bevatten en er niet mee is geknoeid. Ook is de toegang tot gebruikersgegevens vanuit apps beveiligd en wordt dit proces nauwkeurig gecontroleerd.

Dankzij de ingebouwde beveiligingsfeatures ontstaat een stabiel en veilig platform voor apps. Zo kunnen duizenden ontwikkelaars honderdduizenden apps aanbieden voor iOS, iPadOS en macOS, zonder gevaar voor de systeemintegriteit. Gebruikers kunnen deze apps op hun Apple devices gebruiken en zijn beschermd tegen virussen, malware en aanvallen.

Alle apps op iPhone, iPad en iPod touch zijn afkomstig uit de App Store en worden uitgevoerd in een sandbox, wat zorgt voor een optimale beveiliging. Hoewel ook veel Mac-apps afkomstig zijn uit de App Store, kunnen Mac-gebruikers ook apps van internet downloaden en gebruiken. Om veilig materiaal te kunnen downloaden, bevat macOS extra beveiligingslagen. Allereerst moeten alle Mac-apps in macOS 10.15 en hoger door Apple zijn goedgekeurd, anders kunnen ze niet worden geopend. Hierdoor heb je de garantie dat ook apps die niet afkomstig zijn uit de App Store geen bekende malware bevatten. Daarnaast biedt macOS standaard antivirusbescherming conform de standaarden, om malware te blokkeren en indien nodig te verwijderen.

Het gebruik van sandboxes, een extra beveiligingslaag voor alle platforms, voorkomt dat apps zonder toestemming toegang krijgen tot gebruikersgegevens. In macOS worden gegevens binnen kritieke onderdelen standaard in een sandbox geplaatst. De gebruiker bepaalt altijd zelf welke apps toegang krijgen tot bestanden op bijvoorbeeld het bureaublad en in de Documenten- en Downloads-map, zelfs als deze apps niet in een sandbox worden uitgevoerd.

Beveiliging van services

Apple gebruikt robuuste services om devices nog handiger en productiever te maken. Voorbeelden hiervan zijn Apple ID, iCloud, Log in met Apple, Apple Pay, iMessage, FaceTime, Siri en Zoek mijn. Deze services ondersteunen cloudopslag en -synchronisatie, verificatie, betalingen, berichtenverkeer, communicatie en meer, terwijl de privacy en gegevens van de gebruiker beschermd zijn.

Partnerecosysteem

Apple devices ondersteunen bekende zakelijke beveiligingstools en -services, zodat devices en de gegevens daarop volgens de normen zijn beschermd. Elk platform ondersteunt standaardprotocollen voor VPN en wifibeveiliging om het netwerkverkeer te beschermen en veilig verbinding te maken met de infrastructuur van je bedrijf.

Dankzij de samenwerking tussen Apple en Cisco biedt de combinatie van deze systemen extra mogelijkheden voor beveiliging en productiviteit. Cisco Security Connector biedt extra beveiliging bij het gebruik van Cisco-netwerken en geeft bedrijfsapps op deze netwerken voorrang.

Lees meer over de beveiliging van Apple devices.

apple.com/nl/business/it

apple.com/macos/security

apple.com/nl/privacy/features

apple.com/security