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 hardware. Daarom zijn er 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 extra beveiligingsfeatures van de hardware. Goed beveiligde hardware is gestoeld op het principe dat een beperkt en duidelijk gedefinieerd aantal functies wordt ondersteund. Zo wordt de kwetsbaarheid voor aanvallen geminimaliseerd. Denk bijvoorbeeld aan een boot-ROM (een hardwarematige 'Root of Trust' om veilig op te starten), aparte AES-engines voor efficiënte en veilige versleuteling en ontsleuteling en een Secure Enclave.

De Secure Enclave is een system-on-chip (SoC) waarmee alle recente modellen van iPhone, iPad, Apple Watch, Apple TV en HomePod zijn uitgerust, net als de Mac-modellen met Apple Silicon en de Apple T2 Security-chip. De Secure Enclave volgt dezelfde ontwerpprincipes als SoC, met een eigen boot-ROM en AES-engine. De Secure Enclave is ook de basis voor het veilig genereren en bewaren van de sleutels waarmee inactieve gegevens worden versleuteld. Bovendien biedt de Secure Enclave beschermings- en evaluatieopties voor de biometrische gegevens voor Touch ID en Face ID.

Bewaarde gegevens moeten snel en efficiënt worden versleuteld. Tegelijkertijd mogen de gegevens die voor het bepalen van de cryptografische sleutelrelaties ('keying material') worden gebruikt, niet worden ingezien. Daar komt de AES-hardware-engine om de hoek kijken. Bij het wegschrijven of lezen van bestanden

voert deze een snelle in-line versleuteling en ontsleuteling uit. Via een speciaal kanaal van de Secure Enclave wordt de nodige versleutelingsinformatie naar de AES-engine doorgestuurd zonder dat de informatie zelf aan de app-processor (of CPU) of het besturingssysteem wordt doorgegeven. Zo kunnen de Apple Data Protection- en FileVault-technologieën worden ingezet om bestanden te beveiligen zonder dat langdurige coderingssleutels worden doorgegeven.

Apple heeft veilig opstarten zo ontwikkeld dat er niet met de laagste softwareniveaus kan worden geknoeid en dat alleen vertrouwde OS-software van Apple wordt geladen bij het opstarten. Veilig opstarten begint met de onbewerkbare code van het boot-ROM. Deze code, een hardwarematige 'Root of Trust', wordt vastgelegd bij de fabricage van Apple SoC. Op Macs met een T2-chip vormt deze de vertrouwensbasis voor het veilig opstarten van macOS. (Zowel de T2-chip als de Secure Enclave voeren ook hun eigen veilige opstartproces uit op basis van ons boot-ROM. Dit werkt precies hetzelfde als de manier waarop de A-serie en M1-chips veilig opstarten.)

De Secure Enclave verwerkt ook de vingerafdruk- en gezichtsgegevens van de Touch ID- en Face ID-sensors in Apple devices. Zo wordt de identiteit van gebruikers veilig gecontroleerd zonder dat hun biometrische gegevens kunnen worden achterhaald. En profiteren gebruikers van een beveiliging op basis van langere, complexere toegangscodes en wachtwoorden, en kunnen ze zich in de meeste gevallen toch snel aanmelden of afrekenen.

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

Systeembeveiliging
Gebaseerd op de unieke mogelijkheden van Apple hardware, regelt de systeembeveiliging de toegang tot de systeembronnen op Apple devices zonder dat dit ten koste gaat van het gebruiksgemak. De systeembeveiliging omvat de opstartprocedure, de installatie van software-updates en de bescherming van alle bronnen op het computersysteem, zoals de CPU, het geheugen, de harde schijf, software en bewaarde gegevens.

De nieuwste versies van de besturingssystemen van Apple bieden altijd de beste beveiliging. Een belangrijk beveiligingsonderdeel is het proces voor veilig opstarten. Dat voorkomt dat malware het systeem tijdens het opstarten kan binnendringen. 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 tijdig updaten van Apple devices. Subcomponenten als de T2-chip en de Secure Enclave voeren ook hun eigen veilige opstartproces uit om er zeker van te zijn dat alleen vertrouwde code van Apple wordt opgestart. Het updatesysteem kan zelfs downgrade-aanvallen voorkomen, zodat op devices geen eerdere versie van het besturingssysteem kan worden geïnstalleerd (waarmee aanvallers wél raad weten) om gebruikersgegevens te stelen.

Apple devices bieden ook opstart- en runtimebeveiliging voor bescherming van de systeemintegriteit tijdens het gebruik. De door Apple ontwikkelde chips in iPhone, iPad, Apple Watch, Apple TV, en HomePod en de Macs met Apple Silicon vormen een complete architectuur voor het beschermen van de besturingssystemen. Daarnaast beschikt macOS vanwege zijn specifieke verwerkingsmodel ook nog over uitgebreide en aanpasbare beschermingsmogelijkheden plus opties die op alle Macs worden ondersteund.

Versleuteling en beveiliging van gegevens
Apple devices zijn uitgerust met versleutelingsfeatures om gebruikersgegevens te beschermen en devices op afstand te kunnen 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 meer 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 streng 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 met een Intel-processor worden beveiligd met de FileVault-technologie voor volumeversleuteling. Macs met Apple Silicon werken volgens een hybride model dat Data Protection ondersteunt, met twee beperkingen: het laagste beschermingsniveau (klasse D) wordt niet ondersteund en het standaardniveau (klasse C) gebruikt een volumesleutel die hetzelfde werkt als FileVault op een Mac met een Intel-processor. In alle gevallen zijn de hiërarchieën voor sleutelbeheer gebaseerd op de Secure Enclave en zorgt een speciale AES-engine voor versleuteling op lijnsnelheid van bestanden zonder dat langdurige coderingssleutels worden doorgegeven aan het kernelbesturingssysteem of de CPU (waar ze in verkeerde handen kunnen komen). (Een op Intel gebaseerde Mac met een T1-chip of zonder Secure Enclave gebruikt geen speciale chip om de FileVault-coderingssleutels af te schermen.)

De kernel van Apple besturingssystemen gebruikt niet alleen Data Protection en FileVault om ongeoorloofde toegang tot gegevens te voorkomen, maar dwingt ook bescherming en beveiliging af. En plaatst apps met behulp van toegangscontrolefuncties in een sandbox (waardoor de app maar beperkt bij gegevens kan). Verder beperkt een mechanisme dat Data Vault heet de toegang van andere apps tot gegevens op een app (en niet zozeer de verzoeken die een app kan sturen).

Beveiliging van apps
Apps vormen een van de belangrijkste factoren van een 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.

Daarom heeft Apple beveiligingslagen geïmplementeerd om te controleren of apps geen bekende malware bevatten en er niet mee is geknoeid. Ook wordt de toegang tot gebruikersgegevens vanuit apps nauwkeurig gecontroleerd.

Dankzij deze 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 zonder dat ze zich onnodig ongerust hoeven te maken over 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 het 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 nog eens extra afgeschermd. 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. Deze services ondersteunen cloudopslag en synchronisatie, het bewaren van wachtwoorden, authenticatie, betalingen, berichtenverkeer, communicatie en meer, terwijl de privacy en gegevens van de gebruiker beschermd zijn.

Voorbeelden hiervan zijn iCloud, Log in met Apple, Apple Pay, iMessage, Business Chat, FaceTime, ‘Zoek mijn’ en Continuïteit. Hiervoor kan een (beheerde) Apple ID nodig zijn. Voor bepaalde services kunnen geen beheerde Apple ID’s worden gebruikt, bijvoorbeeld bij Apple Pay.

Opmerking: Niet alle Apple services en content zijn in alle landen/regio’s beschikbaar.

Overzicht netwerkbeveiliging
Naast alle ingebouwde beschermingsfeatures voor gegevens op Apple devices kunnen organisaties ook zelf allerlei maatregelen treffen om hun gegevensverkeer zo veilig mogelijk te houden. We hebben het dan over de netwerkbeveiliging.

Gebruikers moeten in de hele wereld toegang hebben tot hun bedrijfsnetwerk. Daarom is het belangrijk om hun toegangsrechten goed te regelen en ervoor te zorgen dat hun gegevens tijdens de overdracht goed worden afgeschermd. Met het oog op die beveiligingseisen worden in iOS, iPadOS en macOS beproefde technologieën en de nieuwste standaarden voor zowel wifi- als mobiele netwerkverbindingen toegepast. Daarom gebruiken onze besturingssystemen standaardnetwerkprotocollen (waartoe ontwikkelaars ook toegang hebben) om ervoor te zorgen dat netwerkcommunicatie wordt geauthenticeerd, geautoriseerd en versleuteld.

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

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 (ook accountgebonden VPN-verbindingen in iOS en iPadOS 14) 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.