Overblik over iOS-sikkerhed

Hos Apple tager vi sikkerheden meget alvorligt, både for brugernes skyld og for at beskytte virksomhedens data. Vi har bygget avanceret sikkerhed ind i vores produkter fra bunden, så de er designet til sikkerhed. Og det har vi gjort på en måde, der er i balance med en fantastisk brugeroplevelse, som giver den enkelte frihed til at arbejde, som han eller hun vil. Kun Apple kan levere et omfattende udvalg af sikkerhedsfunktioner, fordi vi skaber produkter med integreret hardware, software og tjenester.

Designet til sikkerhed

iOS-enheder indeholder avancerede funktioner, der skal beskytte hele systemet, sikre, at alle apps kører på platformen, og sikre, at forretningsmæssige og personlige oplysninger krypteres og administreres problemfrit. Disse funktioner giver omfattende sikkerhed lige fra starten.

Systemsikkerhed. iOS er designet, så både software og hardware er sikker på tværs af alle kernekomponenter i hver enkelt iOS-enhed.

- Fra det øjeblik, hvor enheden tændes, sikrer iOS en sikker opstartsproces. Systemet verificeres ligeledes ved aktivering af enheden.
- iOS gør det nemt for IT-afdelingen at administrere opdateringer af systemsoftwaren for at tage hånd om sikkerhedsproblemer. Alle softwareopdateringer er godkendt til at sikre, at der kun installeres software leveret af Apple.
- Der findes omfattende systemer, herunder politikker for stærke adgangskoder og innovative funktioner, som Touch ID og Face ID, så kun autoriserede brugere kan få adgang til enheden.

Datasikkerhed. iOS leverer robuste og kraftfulde metoder til styring og beskyttelse af data til enhver tid.

- iOS-enheder leveres med en dedikeret hardware-processor og bruger AES-256-kryptering lige fra starten.
- Databeskyttelse på filniveau, som bruger stærke krypteringsnøgler, der er afledt af brugerens unikke adgangskode.
- iOS opretter forbindelse til virksomhedens netværk helt problemfrit og sikkert vha. gennemprøvede teknologier og beskytter data under oprettelsen.

Sikkerhed for apps. En komplet sikkerhedsmodel for iOS-apps, der beskytter mod malware, skadelig kode og frygt for, at data eller fortrolighed uforvarende kunne blive kompromitteret.

- Apple bekræfter identiteten af alle udviklere, inden de kan deltage i et Apple-udviklerprogram.
- Apps i App Store revideres af Apple for at sikre, at de ikke indeholder væsentlige bugs, ikke kompromitterer brugerens anonymitet og opererer i overensstemmelse med klare retningslinjer.
- Interne apps skal underskrives og afgives med et certifikat, der leveres af Apple via Apple-programmet for udviklere i virksomheder (Developer Enterprise Program).
- Med indbygget afviklingsbeskyttelse, sandboxing og rettigheder i iOS kan brugerne downloade, installere og køre apps, vel vidende at de kun tilgår data på autoriserede måder.

Frihed til at arbejde

Der er indbygget omfattende sikkerhed i iOS-enheder, så medarbejderne har frihed til at arbejde. Brugerne kan personligt tilpasse deres enheder, så de kan være endnu mere produktive. Og iOS beskytter brugernes anonymitet, samtidig med at det beskytter og adskiller arbejdsrelaterede og personlige data helt problemfrit.

Individualisering. iOS gør det nemt for brugere at indstille deres egne enheder gennem en simpel, strømlinet proces, der kan automatiseres yderligere ved hjælp af Apples Tilmeldingsordning for enheder (Device Enrollment Program, DEP) og værktøjer til administration af mobile enheder (Mobile Device Management, MDM).

- Med indstillingsassistenten til iOS kan medarbejdere aktivere deres enheder, konfigurere grundlæggende indstillinger og komme i gang med at arbejde med det samme.
- Brugere kan logge ind med deres eget Apple-id for og få en personligt tilpasset oplevelse. Virksomhedsdata sikkerhedskopieres ikke til iCloud, men det gør personlige data. Og de kan desuden finde en mistet enhed med Find min iPhone.

Adskillelse. iOS og MDM kan levere smarte løsninger til diskret at administrere arbejdsdata og -apps, imens arbejdsdata og private data problemfrit adskilles.

- Det er ikke nødvendigt med beholdere eller dobbelte arbejdspladser, der gør brugeren frustreret, og som går ud over brugeroplevelsen.
- Virksomhedskonti, apps, indhold, indstillinger og kontakter, der installeres via en MDM-løsning, anses for at være "administreret" af iOS og kan fjernes af IT-afdelingen til enhver tid, uden at påvirke private data.
- Netværksfunktioner som VPN for hver app sikrer, at trafikken fra virksomhedens apps går via virksomhedens netværk, og at den private trafik går via det offentlige netværk.
- Funktioner som Administreret åbning kan anvendes til at kontrollere strømmen af virksomhedens data mellem apps og forhindre, at dokumenter gemmes i brugerens private apps eller cloud-tjenester. Dette gælder også for dokumentudvidelser fra udbydere.

Anonymitet. Virksomhedsdata forbliver inden for IT-afdelingens kontrol, og personlige data – såsom beskeder, lokalitetsdata, fotos og iCloud-data – forbliver private.

- Apple bygger omfattende sikkerhedssystemer ind i apps, internettjenester og iOS, således at stærke anonymitetsfunktioner konstant arbejder på at beskytte virksomhedens oplysninger.
- Udviklere kan anvende værktøjer som Touch ID API'er, 256-bit-kryptering og app-overførselssikkerhed til at udvikle sikre apps. Apple kræver også, at udviklere beder om tilladelse, inden de tilgår personlige oplysninger som f.eks. kontakter.

Yderligere ressourcer: iOS-sikkerhedsdokument | Face ID-sikkerhedsvejledning | Webside om anonymitet