Apple at Work

Zabezpečení platformy

Bezpečné od základu.

Ve společnosti Apple důsledně dbáme na bezpečnost uživatelů i podnikových dat. Do našich zařízení jsme od základů zabudovali pokročilé zabezpečení, aby byla bezpečná už ze své podstaty. A udělali jsme to způsobem, který je v rovnováze se skvělým uživatelským komfortem, takže uživatelé můžou pracovat přesně tak, jak jim to vyhovuje. Takovýto komplexní přístup k zabezpečení dokáže nabídnout jenom Apple, protože vyvíjí produkty s integrovaným hardwarem, softwarem a službami.

Zabezpečení hardwaru

Bezpečný software vyžaduje, aby byl bezpečný základ zabudovaný do hardwaru. Proto mají zařízení Apple – na kterých běží iOS, iPadOS, macOS, tvOS nebo watchOS – integrované zabezpečení už na úrovni křemíku.

Patří sem speciální vlastnosti procesoru, na kterých strojí systémové bezpečnostní funkce, a taky specializované bezpečnostní čipy. Klíčovou součástí je koprocesor Secure Enclave obsažený ve všech současných zařízeních s iOS, iPadOS, watchOS a tvOS a taky ve všech Macích s čipem Apple T2 Security. Secure Enclave slouží jako základ pro šifrování uložených dat, bezpečné spouštění macOS a biometrické ověřování.

Všechny moderní iPhony, iPady a Macy s čipem T2 obsahují vyhrazený hardwarový engine na AES, který vysokou rychlostí šifruje soubory při čtení nebo zápisu. Díky tomu můžou Ochrana dat a FileVault chránit soubory uživatelů, aniž by procesoru nebo operačnímu systému odhalovaly dlouhodobé šifrovací klíče.

Bezpečné spouštění zařízení Apple zajišťuje, aby software základní úrovně nebyl nijak pozměněný a aby se při spouštění načetl jenom důvěryhodný operační systém od společnosti Apple. V iOS a iPadOS zařízeních začíná zabezpečení neupravitelným kódem zvaným Boot ROM, který integrujeme přímo do čipu už při výrobě – říká se mu hardwarový kořen důvěry („root of trust“). Na Macích s čipem T2 začíná důvěryhodnost bezpečného spouštění u modulu Secure Enclave.

Secure Enclave vyhodnocuje Touch ID a Face ID, na zařízeních Apple tím poskytuje zabezpečené ověřování a zároveň chrání biometrická data a uchovává je důvěrná. Uživatelé si díky tomu můžou nastavit delší a složitější přístupové kódy nebo hesla a v mnoha situacích můžou využít praktické, bleskurychlé ověřování.

Bezpečnostní funkce zařízení Apple vznikají kombinací architektury čipů, hardwaru, softwaru a služeb, jakou může nabídnout jedině Apple.

Zabezpečení systému
Na jedinečných možnostech hardwaru Apple staví zabezpečení systému. Je navržené tak, aby maximalizovalo bezpečnost operačního systému na zařízeních Apple a zároveň zachovalo jednoduchost používání. K zabezpečení systému patří spouštěcí proces, aktualizace softwaru a průběžné fungování operačního systému.

Zabezpečené spouštění začíná u hardwaru a pomocí softwaru pak vytváří řetězec důvěry, kde každý krok kontroluje, jestli následující krok funguje správně, a teprve potom mu předá kontrolu. Tento bezpečnostní model podporuje nejenom výchozí spouštění zařízení Apple, ale i různé další režimy na zotavení nebo aktualizaci zařízení s iOS, iPadOS a macOS.

Nejnovější verze iOS, iPadOS a macOS jsou vždy ty nejbezpečnější. Mechanismus aktualizace softwaru je důležitý nejen proto, že zařízením Apple zajišťuje včasné aktualizace, ale taky proto, že instaluje jenom důvěryhodný software prověřený společností Apple. Aktualizační systém umí dokonce předcházet útokům downgradem – nefungují tedy metody, kdy útočník obnoví na zařízení starší verzi operačního systému a potom z ní ukradne data.

V neposlední řadě obsahují zařízení Apple různé ochrany spouštění a běhu aplikací, které průběžně hlídají jejich integritu. Ochrany se mezi iOS, iPadOS a macOS výrazně liší. Vycházejí totiž z různých schopností zařízení a z rozdílnosti útoků, kterým musí čelit.

Této míry zabezpečení dosahuje iOS a iPadOS tím, že používá ochranu integrity jádra, integritu systémového koprocesoru, kódy na ověřování ukazatelů a vrstvu ochrany stránky. macOS používá zabezpečení jednotného rozhraní rozšiřitelného firmwaru, režim správy systému, ochranu přímého přístupu k paměti a zabezpečení periferního firmwaru.

Šifrování a ochrana dat
Zařízení Apple mají šifrovací funkce, které chrání data uživatelů a v případě ztráty nebo krádeže umožňují vymazání dat na dálku.

Zabezpečený spouštěcí řetězec, zabezpečení systému a funkce na zabezpečení aplikací společně hlídají, aby na zařízení běžel jenom důvěryhodný kód a aplikace. Zařízení Apple mají další šifrovací funkce na ochranu uživatelských dat i v případě, že byly narušeny jiné části bezpečnostní infrastruktury – například když se zařízení ztratí nebo na něm běží nedůvěryhodný kód. Tyto funkce pomáhají uživatelům i správcům IT, protože neustále chrání osobní i firemní informace a poskytují nástroje na okamžité a kompletní vymazání zařízení na dálku v případě ztráty nebo krádeže.

iOS a iPadOS zařízení používají metodologii šifrování souborů zvanou Ochrana dat, zatímco data na Macu jsou chráněna technologií šifrování svazku zvanou FileVault. Oba modely se podobají tím, že hierarchii správy klíčů opírají o funkce integrované přímo do čipu Secure Enclave (na zařízeních obsahujících SEP). Oba modely taky používají specializovaný engine na AES, který podporuje šifrování vysokou přenosovou rychlostí a zajišťuje, že dlouhodobé šifrovací klíče se nikdy nemusí odhalit procesoru ani jádru operačního systému, kde by mohly být zneužity.

Zabezpečení aplikací

K nejzranitelnějším prvkům moderní bezpečnostní architektury patří aplikace. Uživatelům sice otevírají skvělé pracovní možnosti, ale zároveň mají potenciál negativně ovlivňovat zabezpečení systému, stabilitu a uživatelská data – tedy pokud se s nimi nezachází správně. Apple používá vrstvy ochrany, které zajišťují, aby aplikace neobsahovaly známý malware a nebyly modifikované. Další ochrany hlídají, jestli má aplikace přístup ke všem uživatelským datům, a pečlivě tento proces střeží.

Vestavěné bezpečnostní funkce poskytují bezpečnou stabilní platformu pro aplikace, díky které můžou tisíce vývojářů zpřístupňovat statisíce aplikací pro iOS, iPadOS a macOS, aniž by jakkoli ohrozili integritu systému. Uživatelé pak můžou s aplikacemi pracovat, zatímco bezpečnostní funkce je chrání před viry, malwarem a neoprávněnými útoky.

Na iPhonu, iPadu a iPodu touch se všechny aplikace instalují z App Storu – a všechny běží v sandboxu, aby ochrana byla maximální. Na Macu se velká část aplikací stahuje taky z App Storu, ale kromě toho si uživatelé Macu můžou aplikace stahovat i z internetu. macOS má proto další funkce, které zaručují bezpečné stahování z internetu. Především se aplikace pro Mac v macOS 10.15 a novějším nespustí, pokud nemají notarizaci od společnosti Apple. Tento požadavek zaručuje, že aplikace nebudou obsahovat známý malware – a zároveň není nutné, aby byla aplikace distribuována přes App Store. Navíc macOS obsahuje antivirové ochrany na úrovni oborových standardů, které blokují a případně odstraňují škodlivý software.

Další bezpečnostní funkcí na všech platformách je sandboxing, díky kterému nemůžou aplikace neoprávněně přistupovat k uživatelským datům. V macOS jsou do sandboxu pro všechny aplikace uzavřená i data v kritických umístěních, takže soubory na ploše, v Dokumentech, ve složce Stahování i na jiných místech jsou zabezpečené nehledě na to, jestli aplikace, která se k nim snaží přistupovat, běží v sandboxu, nebo ne.

Zabezpečení služeb

Apple vyvinul širokou škálu služeb, které uživatelům pomáhají mít ze zařízení ještě větší užitek a být díky nim ještě produktivnější. Patří k nim Apple ID, iCloud, Přihlášení přes Apple, Apple Pay, iMessage, FaceTime, Siri a aplikace Najít. Tyto služby nabízejí užitečné funkce na ukládání dat do cloudu, synchronizaci, ověřování, platby, posílání práv, komunikaci a mnohem víc. Zároveň chrání soukromí uživatelů a bezpečnost jejich dat.

Partnerský ekosystém

Zařízení Apple spolupracují s běžnými firemními nástroji a službami, aby zařízení i v nich uložená data vyhovovala potřebným standardům. Každá platforma podporuje standardní protokoly pro VIP a zabezpečení Wi-Fi, které chrání síťový provoz a umožňují bezpečné připojování ke společné firemní infrastruktuře.

Partnerství mezi společnostmi Apple a Cisco usiluje o lepší zabezpečení a vyšší produktivitu. Sítě Cisco poskytují lepší zabezpečení prostřednictvím Cisco Security Connectoru. A podnikové aplikace mají v sítích Cisco prioritu.

Přečtěte si víc o zabezpečení zařízení Apple.

apple.com/cz/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/cz/security