Apple w pracy

Bezpieczeństwo całej platformy

Urządzenia z natury bezpieczne.

Apple troszczy się o bezpieczeństwo zarówno w przypadku użytkowników, jak i należących do przedsiębiorstw danych. Zaawansowane zabezpieczenia uwzględniamy już w podstawowych założeniach konstrukcyjnych naszych produktów. Zawsze dbamy o to, aby skuteczna ochrona nie kolidowała z komfortem pracy użytkowników, a wszyscy mogli swobodnie pracować tak, jak chcą. W Apple tworzymy produkty, w których sprzęt, oprogramowanie i usługi są ze sobą zintegrowane, więc jako jedyni możemy podchodzić do kwestii bezpieczeństwa tak kompleksowo.

Bezpieczeństwo sprzętu
Bezpieczne oprogramowanie wymaga fundamentu w postaci wbudowanych w sprzęt zabezpieczeń. Dlatego urządzenia Apple — z systemami iOS, iPadOS, macOS, tvOS lub watchOS — są chronione już na poziomie układów scalonych.

Procesor główny (CPU) oferuje specjalnie zaprojektowane funkcje zabezpieczające i współpracuje z układami odpowiedzialnymi za bezpieczeństwo. Najistotniejszym komponentem oferowanych obecnie urządzeń iOS, iPadOS, watchOS i tvOS oraz wszystkich komputerów Mac z czipem Apple T2 Security jest koprocesor Secure Enclave, używany do szyfrowania danych w spoczynku, bezpiecznego uruchamiania systemu macOS i obsługi funkcji biometrycznych.

Wszystkie najnowsze iPhone'y, iPady i komputery Mac z czipem T2 wykorzystują sprzętowy układ AES do błyskawicznego szyfrowania zapisywanych lub odczytywanych plików. Dzięki temu funkcje ochrony danych i FileVault zabezpieczają pliki użytkowników, nie ujawniając długotrwale przechowywanych kluczy szyfrowania procesorowi ani systemowi operacyjnemu.

Bezpieczne uruchamianie urządzeń Apple gwarantuje, że oprogramowanie nie zostanie zmodyfikowane na najniższym poziomie, a podczas startu ładowany jest wyłącznie zaufany system operacyjny Apple. Jeśli chodzi o urządzenia iOS i iPadOS, fundament zabezpieczeń stanowi niezmienny kod, tak zwany Boot ROM, implementowany na etapie produkcji czipu, stanowiący główny aparat zaufania (root of trust). W przypadku komputerów Mac z czipem T2 za bezpieczne uruchamianie systemu odpowiada sam koprocesor Secure Enclave.

Koprocesor Secure Enclave umożliwia funkcjom Touch ID i Face ID dostępnym w urządzeniach Apple bezpieczne uwierzytelnianie użytkowników, a jednocześnie ochronę prywatności i poufności ich danych biometrycznych. Dzięki temu użytkownicy z jednej strony są chronieni przez dłuższe, bardziej złożone kody dostępu i hasła, a z drugiej dysponują przydatną w wielu sytuacjach możliwością szybkiego uwierzytelniania tożsamości.

Zabezpieczenia urządzeń Apple to połączenie unikatowych, oferowanych tylko przez Apple rozwiązań półprzewodnikowych, sprzętowych i programowych oraz usług.

Bezpieczeństwo systemu

Zabezpieczenia systemu — oparte na wyjątkowych możliwościach sprzętu Apple — zapewniają najwyższy poziom ochrony systemów operacyjnych urządzeń Apple, w żaden sposób nie umniejszając wygody ich użytkowania. Zabezpieczenia działają zarówno podczas uruchamiania i aktualizowania systemu operacyjnego, jak i w trakcie jego codziennego działania.

Bezpieczne uruchamianie rozpoczyna się już na poziomie sprzętu. Dalej w budowę „łańcucha zaufania" włącza się oprogramowanie — przed oddaniem sterów użytkownikowi poprawność funkcjonowania każdego kolejnego etapu kontrolują etapy go poprzedzające. Ten model zabezpieczeń towarzyszy nie tylko uruchamianiu urządzeń Apple, ale także różnym trybom odzyskiwania i aktualizowania urządzeń iOS, iPadOS i macOS.

Najnowsze wersje systemów iOS, iPadOS i macOS są najbezpieczniejsze. Mechanizm aktualizacji oprogramowania ułatwia nadążanie za uaktualnieniami urządzeń Apple, a także dostarcza wyłącznie zaufane oprogramowanie od Apple. System aktualizacji zapobiega nawet atakom typu downgrade, uniemożliwiając przywracanie starszych wersji systemu operacyjnego w celu kradzieży danych użytkowników.

Urządzenia Apple dysponują zabezpieczeniami środowiska uruchamiania i środowiska wykonawczego, dzięki czemu są stale chronione podczas bieżącej pracy. Na urządzeniach iOS, iPadOS i macOS zabezpieczenia te wyglądają różnie. Zależą przede wszystkim od funkcji i możliwości, którym towarzyszą, oraz rodzajów potencjalnych ataków, którym muszą zapobiegać.

W celu zapewnienia bezpieczeństwa na tak wysokim poziomie urządzenia iOS i iPadOS wykorzystują technologie ochrony integralności jądra (Kernel Integrity Protection), ochrony integralności koprocesora systemowego (System Coprocessor Integrity), kody uwierzytelniania wskaźników (Pointer Authentication Codes) i warstwę ochrony stron (Page Protection Layer). Natomiast system macOS polega standardzie UEFI (Unified Extensible Firmware Interface), trybie zarządzania systemem (System Management Mode), zabezpieczeniach bezpośredniego dostępu do pamięci i zabezpieczeniach oprogramowania sprzętowego urządzeń peryferyjnych.

Szyfrowanie i ochrona danych

Urządzenia Apple wyposażono w funkcje szyfrowania, które chronią dane użytkowników i umożliwiają ich zdalne wymazywanie w przypadku kradzieży lub zgubienia urządzenia.

Bezpieczne uruchamianie, zabezpieczenia systemu oraz mechanizmy ochrony aplikacji pozwalają zyskać pewność, że na urządzeniu działają wyłącznie sprawdzone aplikacje i zaufany kod. Urządzenia Apple oferują dodatkowe funkcje szyfrowania, które chronią dane użytkowników, nawet jeśli inne obszary infrastruktury zabezpieczeń zawiodły — na przykład gdy doszło do zgubienia

urządzenia lub uruchomienia niezaufanego kodu. Wszystkie te rozwiązania przynoszą korzyści zarówno użytkownikom, jak i administratorom IT. Nieprzerwanie chronią dane osobowe i informacje firmowe, a także umożliwiają natychmiastowe i całkowicie zdalne wymazywanie pamięci w przypadku kradzieży lub zgubienia urządzenia.

Urządzenia iOS i iPadOS wykorzystują metodę szyfrowania plików, nazywaną w systemie ochroną danych. Z kolei dane na komputerach Mac są chronione za pośrednictwem szyfrującej woluminy technologii FileVault. W obu przypadkach hierarchie zarządzania kluczami bazują na specjalnym układzie scalonym — koprocesorze Secure Enclave znajdującym się w urządzeniach obsługujących technologię SEP. Ponadto oba modele urządzeń wyposażono w specjalny mechanizm AES, który umożliwia błyskawiczne szyfrowanie i długotrwałe przechowywanie kluczy bez konieczności przekazywania ich do jądra systemu operacyjnego lub procesora, gdzie istnieje ryzyko ich przechwycenia.

Zabezpieczenia aplikacji
Aplikacje to jeden z najbardziej newralgicznych elementów nowoczesnej architektury zabezpieczeń. Z jednej strony aplikacje znacznie zwiększają wydajność pracy użytkowników, a z drugiej — ich niewłaściwe użytkowanie niesie za sobą potencjalne zagrożenia dla bezpieczeństwa systemu, stabilności i danych użytkowników. Apple oferuje kilka warstw ochrony, które pozwalają zyskać pewność, że aplikacje są wolne od znanego szkodliwego oprogramowania i niepożądanych modyfikacji. Dodatkowe zabezpieczenia zarządzają dostępem aplikacji do wszelkich danych użytkowników i ściśle monitorują ten proces.

Wbudowane mechanizmy kontroli dostępu zapewniają stabilną i bezpieczną platformę dla aplikacji, która pozwala tysiącom deweloperów tworzyć setki tysięcy aplikacji dla systemów iOS, iPadOS czy macOS — bez negatywnego wpływu na integralność systemu. Ponadto podczas korzystania z tych aplikacji na urządzeniach Apple użytkownikom towarzyszą mechanizmy chroniące przed wirusami, szkodliwym oprogramowaniem czy nieautoryzowanym dostępem.

Na iPhonie, iPadzie i iPodzie touch wszystkie aplikacje — z których każda działa w piaskownicy — uzyskuje się ze sklepu App Store. Pozwala to sprawować nad nimi ścisłą kontrolę. Z kolei użytkownicy Maca znajdą wiele aplikacji w sklepie App Store, ale mogą także pobierać i wykorzystywać aplikacje z Internetu. Aby zadbać o bezpieczeństwo w przypadku pobierania aplikacji z Internetu, system macOS wykorzystuje dodatkowe mechanizmy. Po pierwsze, począwszy od systemu macOS 10.15 wszystkie aplikacje na Maca muszą zostać poświadczone przez Apple przed uruchomieniem. To gwarancja, że są wolne od znanego szkodliwego oprogramowania, mimo braku dystrybucji za pośrednictwem App Store. System macOS wykorzystuje też zgodne ze standardami branżowymi oprogramowanie antywirusowe do blokowania, a w razie potrzeby również usuwania szkodliwego oprogramowania.

Dodatkowy mechanizm zabezpieczeń na różnych platformach stanowi piaskownica, która pomaga chronić dane użytkowników przed nieuprawnionym dostępem aplikacji. W systemie macOS dane znajdujące się w newralgicznych obszarach także trafiają do piaskownicy. Dzięki temu użytkownicy mają pełną kontrolę nad dostępem wszystkich aplikacji do plików z folderów Biurko, Dokumenty, Pobrane rzeczy i innych miejsc bez względu na to, czy same aplikacje również znajdują się w piaskownicy, czy też nie.

Bezpieczeństwo usług
Apple oferuje wszechstronną gamę usług, które pomagają użytkownikom wykorzystywać jeszcze więcej możliwości urządzeń i osiągać jeszcze lepszą produktywność. Usługi te to m.in. Apple ID, iCloud, Zaloguj się przez konto Apple, Apple Pay, iMessage, FaceTime, Siri i Lokalizator. Zapewniają one szeroki wachlarz zaawansowanych możliwości, takich jak przechowywanie i synchronizowanie

danych w chmurze, uwierzytelnianie, płacenie, wysyłanie wiadomości czy komunikowanie się. Jednocześnie chronią prywatność użytkowników i zabezpieczają ich dane.

Ekosystem partnerów

Urządzenia Apple współpracują z powszechnie wykorzystywanymi w przedsiębiorstwach narzędziami i usługami w dziedzinie bezpieczeństwa. Gwarantują zgodność urządzeń i znajdujących się na nich danych z obowiązującymi wymogami. Każda platforma obsługuje standardowe protokoły sieci VPN i bezpiecznej sieci Wi-Fi, tak by chronić ruch sieciowy i w bezpieczny sposób zapewniać dostęp do wspólnej infrastruktury korporacyjnej.

Współpraca Apple z Cisco przekłada się na wyższy poziom bezpieczeństwa i wydajności współpracujących produktów obu firm. Sieci Cisco zapewniają lepszą ochronę dzięki rozwiązaniu Cisco Security Connector i przyznają pierwszeństwo aplikacjom biznesowym.

Dowiedz się więcej o bezpieczeństwie urządzeń Apple.

apple.com/pl/business/it

apple.com/macos/security

apple.com/privacy/features

apple.com/pl/security