MacBook w biznesie

Bezpieczeństwo

INNERGO systems

Authorised Enterprise Reseller

Bezpieczeństwo i łatwość zarządzania, czyli platforma macOS w firmie

Wymiana czy zakup nowego sprzętu komputerowego dla pracowników jest dużym przedsięwzięciem, wiążącym się nie tylko z kosztami, ale też z instalowaniem aplikacji, integracją czy migracją danych, ustawieniem odpowiednich dostępów, haseł, zapewnieniem bezpieczeństwa danych użytkowników i firmy.

> To wyzwanie i dla zarządów, i dla działów IT. Wyzwanie, które może zaangażować zasoby przedsiębiorstwa na długie tygodnie lub doprowadzi do stworzenia w firmie nowej i intuicyjnej infrastruktury, którą łatwo zarządzać. Tę drugą sytuację umożliwia zastosowanie komputerów Mac oraz platformy macOS.

Integracja sprzętu, oprogramowania i usług. To elementy platformy macOS, dzięki którym system jest bezpieczny, łatwy w konfiguracji, a przy okazji przyjazny podczas wdrażania i prosty w codziennym zarządzaniu. Sama platforma składa się z zestawu funkcji i usług, na które powinien zwrócić uwagę każdy, komu zależy na zwiększeniu bezpieczeństwa w firmie.

To również pakiet najbardziej zaawansowanych technologii i funkcji, który zapewnia z jednej strony działanie w pełni bezpiecznej architektury, a z drugiej swobodę podczas użytkowania urządzeń.

BEZPIECZŃSTWO

Które funkcje i rozwiązania techniczne środowiska macOS pomogają zapewnić odpowiednią ochronę danych w środowisku korporacyjnym?

Czip Apple T2 z modułem Secure Enclave

Pierwszym istotnym zabezpieczeniem jest **czip Apple T2** z modułem **Secure Enclave**, który chroni informacje o odcisku palca używanym do identyfikacji użytkownika. Czytnik **Touch ID** zapewnia szybki i łatwy, a zarazem bezpieczny dostęp do urządzenia. Dzięki niemu zastosowanie dłuższego i bardziej złożonego kodu bezpieczeństwa jest znacznie praktyczniejsze, ponieważ użytkownik dużo rzadziej musi go wpisywać. Oprócz tego Touch ID pozwala obejść niedogodności wynikające z blokowania komputera hasłem. Nie zastępuje go jednak, ale zapewnia bezpieczny dostęp, w którym uwzględnione są odpowiednie ograniczenia czasowe. Wspomniany wcześniej czip zabezpieczeń Apple T2 jest również fundamentem nowej funkcji szyfrowania dysku i bezpiecznego rozruchu.

Aktualizacje oprogramowania

Najnowsze oprogramowanie to jeden z najskuteczniejszych sposobów na bezpieczeństwo komputerów. Ogromną wartością systemu macOS jest to, że jego aktualizacje dostępne są zupełnie bezpłatnie i dzięki specjalnemu mechanizmowi kontroli można wymusić je na wszystkich firmowych komputerach. Działom IT daje to pewność, że sprzęt pozostaje pod stałą ochroną, a pracownikom – możliwość swobodnego korzystania z najnowszych funkcji bez ryzyka utraty danych.

Szyfrowanie danych

Coraz częściej rozmowy biznesowe przenoszą się z tradycyjnych kanałów do usług Apple. Nie ma chyba dziś wśród nas już nikogo, kto nie przekazywałby nigdy za pośrednictwem Face Time czy iMessage informacji poufnych lub objętych tajemnicą handlową. Na szczęście usługi te zaprojektowane są tak, aby połączenia były zaszyfrowane na całej drodze przesyłu. Nie ma więc możliwości odszyfrowania treści rozmowy w trakcie jej transmisji między urządzeniami. Wszystko dzięki temu, że Mac obsługuje wiele popularnych standardów sieciowych i **zabezpieczeń sieci**.

> Jeśli firma używa jednego z tych protokołów, nie musi przeprowadzać dodatkowej konfiguracji sieci ani nie potrzebuje aplikacji innych firm. iOS i macOS obsługują oferowane przez popularnych dostawców technologii VPN rozwiązania korzystające z protokołu SSL VPN.

Wolumin systemowy przeznaczony tylko do odczytu

Ciekawym rozwiązaniem zabezpieczającym w macOS jest funkcja **woluminu systemowego przeznaczonego tylko do odczytu**. Zapobiega modyfikowaniu systemu operacyjnego i jest efektem rozwinięcia prac nad mechanizmem ochrony jego integralności (SIP, System Integrity Protection). Jak działa ta funkcja? Dzięki możliwości utworzenia odrębnego

woluminu APFS przeznaczonego na system macOS pliki systemowe mogą zostać odseparowane od wszystkich pozostałych danych w komputerze Mac. Efekt? Brak ryzyka przypadkowego nadpisania newralgicznych plików systemowych.

Funkcja FileVault 2

Z kolei dzięki funkcji **FileVault 2** firma może mieć pewność, że dane zlokalizowane na komputerze pracownika będą bezpieczne nawet wówczas, gdy Mac dostanie się w niepowołane ręce. FileVault 2 szyfruje całą zawartość dysku komputera Mac, zabezpieczając dane przy użyciu algorytmu XTS-AES 128. Co więcej, w komputerach Mac z czipem Apple T2 klucze FileVault 2 są tworzone i zabezpieczane przez wspomniany już wyżej Secure Enclave. Włączenie funkcji FileVault spowoduje, że przed uruchomieniem urządzenia pracownik będzie proszony o podanie hasła. Klucze odzyskiwania dla FileVault można przechowywać w rozwiązaniu MDM, które pozwala również między innymi na zdalne aktywowanie tej funkcji.

Instalacja zaufanych aplikacji

Aplikacje to jeden z najbardziej newralgicznych elementów nowoczesnej architektury IT, ponieważ ich niewłaściwe używanie niesie ze sobą wiele potencjalnych zagrożeń. macOS zawiera wbudowane rozwiązania techniczne, które dbają o instalowanie wyłącznie zaufanych aplikacji oraz pomagają w obronie przed złośliwym oprogramowaniem. Aby wykluczyć niedozwolone modyfikacje bezpiecznych aplikacji, macOS wyposażony jest w warstwową architekturę ochrony środowiska wykonawczego oraz podpisywania aplikacji. Należą do niej między innymi tzw. **funkcja XD** (blokada wykonania), losowe wykorzystanie przestrzeni adresowej (Address Space Layout Randomization, ASLR) i ASLR, które utrudniają złośliwemu oprogramowaniu działanie i wyrządzanie szkód w pamięci operacyjnej lub aplikacjach. Ważną funkcję pełni też ochrona integralności systemu (System Integrity Protection, SIP), uniemożliwiająca modyfikowanie najważniejszych plików i ustawień systemowych.

Istotnym „strażnikiem aplikacji" jest **Gatekeeper**, pozwalający określać źródła, z których mogą być instalowane aplikacje. Prościej mówiąc, dba o to, żeby każda nowo instalowana aplikacja była przed uruchomieniem sprawdzona pod kątem znanych zagrożeń bezpieczeństwa. Dużą wygodą – szczególnie dla organizacji – jest możliwość definiowania poziomu zabezpieczeń obowiązującego przy instalacji aplikacji. Funkcja Gatekeeper pozwala uruchamiać je nie tylko z Mac App Store, ale także z innych źródeł, o ile – co ważne – zostały podpisane identyfikatorem programisty wydanym przez Apple, czyli przeszły kontrolę bezpieczeństwa, inaczej notaryzację.

Ponadto, wszystkie aplikacje z App Store funkcjonują w piaskownicy (ang. sandbox), która dba o to, by działały one zgodnie ze swoim przeznaczeniem. Piaskownica oddziela aplikacje od kluczowych komponentów systemu na Macu pracownika, danych oraz innych aplikacji. A to oznacza, że nawet jeśli szkodliwe oprogramowanie zaatakuje aplikację, piaskownica automatycznie je zablokuje. Oprócz tego macOS daje

pracownikowi kontrolę nad tym, które aplikacje mają dostęp do jego kalendarza, kontaktów, zdjęć, lokalizacji, przypomnień i prywatnych danych systemowych, takich jak historia wiadomości, baza danych aplikacji mail lub przeglądarki Safari oraz kamer czy mikrofonu.

Warto wrócić jeszcze do wspomnianej wcześniej **notaryzacji aplikacji**. To usługa, dzięki której programiści mogą przesyłać aplikacje do Apple'a, aby zostały sprawdzone przed ich dystrybucją. Gdy użytkownicy macOS po raz pierwszy otworzą aplikację, Gatekeeper wyświetli komunikat, który da im pewność, że aplikacja nie jest złośliwym oprogramowaniem. Sprawdzone aplikacje podpisane są certyfikatem ID dewelopera i zawierają potwierdzenie od Apple'a wymagane są również systemowo w najnowszych wersjach macOS. Oczywiście, dział IT za pośrednictwem systemu MDM może określić, czy dana aplikacja wymaga notaryzacji. Jeśli nie jest ona konieczna lub możliwa, aplikację można wpisać na tzw. białą listę systemu MDM i tym samym ominąć obowiązek notaryzacji.

Interfejsy API

Kolejną formą zabezpieczenia są **rozszerzenia systemowe**, czyli interfejsy API. Dlaczego? Ponieważ umożliwiają twórcom zabezpieczeń punktów końcowych, aplikacji sieciowych, plików, sterowników drukarek czy skanerów budowanie oprogramowania działającego poza jądrem systemu. Zamiast używać stosowanych obecnie rozszerzeń jądra (KEXT), mogą wykorzystać rozszerzenia, nie narażając jądra systemu. W związku z tym działy IT powinny wybierać produkty dostawców, którzy stosują tego typu rozwiązania.

Blokada aktywacji

Warto zwrócić uwagę jeszcze na **blokadę aktywacji**, działającą na komputerach Mac z czipem T2 i oferującą te same zabezpieczenia, które są już dostępne w systemie iOS. Funkcją można zarządzać za pośrednictwem systemu MDM – zezwalać na jej używanie, włączać ją i generować kody potrzebne do obejścia blokady. Aby było to możliwe, komputer musi być objęty nadzorem, czyli zarejestrowany za pomocą usługi **Apple Business Manager**.

ZARZĄDZANIE

Jak zarządzać komputerami Mac w organizacji?

Najlepiej robić to, wykorzystując systemy Mobile Device Management takich firm jak VMware czy Jamf, które najczęściej zintegrowane są z usługą **Apple Business Manager**.

Apple Business Manager to prosty w obsłudze portal, który pozwala zespołom IT zarządzać urządzeniami, kupować i rozpowszechniać treści oraz administrować firmowymi Apple IDs pracowników.

Rejestrowanie urządzeń

Rejestrowanie urządzeń odbywa się w portalu i pozwala na ekspresowe wdrożenie komputerów Mac.. Administratorzy mają do dyspozycji opcję ustawiania różnych typów serwerów MDM dla różnych typów urządzeń – innych dla Maców, iPhonów czy iPadów.

Książki, aplikacje znajdują się w jednym miejscu portalu, z którego firma może hurtowo nabywać treści. Licencje na nie da się bezproblemowo współużytkować w ramach jednej lokalizacji lub dowolnie przenosić pomiędzy nimi. Portal umożliwia tworzenie nowych firmowych kont Apple ID. Konta pomagają w aktywacji urządzeń, zarządzaniu tożsamością, sprzętem i treścią w portalu.

W nowych wersjach systemu Apple wprowadza możliwość **modyfikowania procesu rejestracji**, która pozwala na wzbogacenie procesu udostępniania nowych urządzeń. Zapewnia to przede wszystkim jeszcze lepsze doświadczenie użytkowników i możliwość zabezpieczenia procesu konfiguracji za pomocą używanych dotychczas w firmie usług uwierzytelniania, np. Azure Active Directory czy innych.

Jak to działa?

Administrator IT za pośrednictwem arkuszy WWW wprowadza do interfejsu użytkownika elementy własnej marki, teksty zgód czy wspomniane wcześniej stosowane w firmie już kiedyś mechanizmy uwierzytelnienia. W tym ostatnim przypadku doskonale sprawdza się uwierzytelnianie federacyjne, czyli zarządzanie tożsamościami, które można zintegrować z istniejącą infrastrukturą organizacji. Pracownicy uzyskują w ten sposób dostęp do pełnego ekosystemu Apple bez konieczności zapamiętywania jeszcze jednego zestawu poświadczeń.

Separacja danych służbowych i prywatnych

Separacja danych i aplikacji służbowych od prywatnych zasobów użytkownika to kolejny bardzo ważny krok zapewniający bezpieczeństwo danych osobowych. Apple Business Manager udostępnia mechanizmy separacji danych, które skutecznie oddzielają od siebie prywatne konta Apple ID od tych firmowych.

Pojedyncze logowanie do aplikacji i witryn

Dzięki architekturze ogólnosystemowych rozszerzeń do **pojedynczego logowania (SSO)**, która jest częścią najnowszych systemów Apple, deweloperzy mogą tworzyć rozszerzenia obsługujące zarówno aplikacje natywne, jak i Safari. Jakie możliwości daje ta funkcja? Przede wszystkim wygodę. Po pierwsze dla użytkowników, którzy tylko raz muszą logować się do jednej z aplikacji lub witryn korporacyjnych. Po drugie dla zespołów IT, ponieważ omawiana funkcja umożliwia zaawansowane uwierzytelnienie wieloczynnikowe w aplikacjach lub witrynach WWW z wykorzystaniem usług dostawcy tożsamości. Obsługa pojedynczego logowania wraz z odpowiednią architekturą dla deweloperów wbudowana jest w każdy system operacyjny. Konfiguruje się ją za pośrednictwem systemu MDM. Pojedyncze logowanie korzysta z dodatkowego rozwiązania, czyli domen skojarzonych. To specjalny mechanizm pozwalający na stosowanie tych samych rozwiązań w aplikacjach opracowanych wewnętrznie i zarządzanie nimi przez system MDM. Odpowiedni, nowy pakiet MDM konfiguruje domeny skojarzone, używane z takimi funkcjami jak rozszerzalne pojedyncze logowanie, łącza uniwersalne i autowypełnianie haseł.

Kolejną, ważną częścią architektury pojedynczego logowania jest **rozszerzenie Kerberos**. Umożliwia łatwe integrowanie urządzeń organizacji z usługą Active Directory – pozwala zarządzać hasłami i synchronizować hasła lokalne. Obsługuje też uwierzytelnianie za pomocą inteligentnych kart i certyfikatów.

Zdalna konfiguracja urządzenia użytkownika końcowego

Dzięki systemom takim jak Mobile Device Management w łatwy sposób można również **skonfigurować urządzenie użytkownika końcowego** – zdalnie zainstalować aplikację lub ją usunąć, przysłać ustawienia np. klienta pocztowego, skonfigurować Wi-Fi, wymusić uaktualnienie do najnowszej wersji oprogramowania systemowego lub wyegzekwować standardy bezpieczeństwa obowiązujące w konkretnej organizacji.