

MATERIAŁ PRODUKTOWY

Systemy EMM i Rozwiązania Apple

Systemy EMM i Rozwiązania Apple

Obecnie niemal w każdej firmie pracownicy korzystają ze smartfonów i tabletów, na których sprawdzają służbową pocztę i otwierają dokumenty. W związku z tym, praktycznie każde urządzenie mobilne jest źródłem wrażliwych danych o nas i naszej działalności biznesowej, od dokumentów, po loginy i hasła.

Niezabezpieczony smartfon, czy tablet, który wpadł w niepowołane ręce, wiąże się z ogromnym ryzykiem. Wystarczy sobie wyobrazić, że nieuwierzytelniony użytkownik ma nieograniczony dostęp do służbowej korespondencji mailowej, w której znajdzie wszystkie informacje biznesowe na temat naszej działalności lub korzysta z dostępu do portali bankowych i potwierdzeń SMS, które najczęściej skonfigurowane są z poziomu tego samego urządzenia. Tylko te kilka przykładów dają do zrozumienia, z jakimi zagrożeniami mamy do czynienia.

W odpowiedzi na te zagrożenia powstały systemy do zarządzania urządzeniami mobilnymi MDM [Mobile Device Management], które już teraz ewoluowały w platformy do zarządzania mobilnością przedsiębiorstwa EMM [Enterprise Mobility Management]. Tego rodzaju systemy przede wszystkim zabezpieczają urządzenia przenośne, aby osoby postronne nie miały dostępu do wrażliwych danych, znajdujących się na smartfonie lub tablecie. EMM daje użytkownikom mobilnym możliwość bezpiecznego, kontrolowanego, ale i przystępnego dostępu do kluczowych danych w każdej chwili, niezależnie od miejsca, w którym się znajdują. Natomiast administratorom IT oferuje wiele funkcjonalnych i skutecznych narzędzi do zarządzania i wsparcia floty urządzeń mobilnych.

Systemy EMM i mobilność przedsiębiorstw

Rynek każdej branży wymaga obecnie różnych narzędzi do zarządzania. Korzystamy z wielu różnych systemów do zarządzania klientami, urządzeniami, tożsamością, aplikacjami, czy wirtualizacją.

Te wszystkie narzędzia można połączyć w celu stworzenia jednego cyfrowego miejsca pracy, które obok łączności i aplikacji mobilnych, ma największą wartość dla biznesu, gdyż koncentruje się na użytkowniku. Z pomocą przychodzi tutaj VMware Workspace ONE, oferując jeden system do zarządzania m.in. tożsamością, informacjami osobistymi, punktami końcowymi. Dzięki temu rozwiązaniu użytkownik otrzymuje dostęp do każdej aplikacji z poziomu każdego urządzenia. Częścią pakietu Workspace ONE jest rozwiązanie EMM VMware AirWatch.

Jeśli pracownik ma możliwość korzystania z urządzeń służbowych w celach prywatnych, VMware AirWatch pomaga w oddzieleniu zasobów pracy od zasobów osobistych.

Oddziela on aplikacje wykorzystywane w pracy i prywatnie, zapobiega przepływowi danych między nimi, a dodatkowo zezwala działowi IT tylko na zarządzanie i zabezpieczanie aplikacji i danych związanych z pracą, szanując prywatność pracowników.

Istnieją aplikacje VMware AirWatch, które dodatkowo zabezpieczą i zoptymalizują pracę na urządzeniach mobilnych:

- Boxer – dostęp do poczty firmowej w bezpiecznym i intuicyjnym kontenerze
- Content Locker – dostęp i zabezpiecza zawartości firmowe
- Browser – bezpieczne przeglądanie Intranetu i aplikacji sieci Web
- Socialcast – dostęp do chronionego grupowego czatu firmowego

Dzięki systemowi EMM, dział IT ma możliwość zarządzania różnymi punktami końcowymi [np. smartfonami, tabletami, laptopami, drukarkami, smartwatchami], obsługiwany przez różnych użytkowników. Administratorzy IT w zdalny sposób konfiguruje urządzenie, przygotowując je do użycia, wprowadzają aktualizacje, śledzą zasoby, ustalają zasady i ustawienia bezpieczeństwa. Dzięki tym możliwościom systemy EMM wspierają pełny cykl życia aplikacji od zabezpieczenia, przez aktualizację, aż po analizę.

Skuteczność działań IT znacznie wzrasta ze względu na oszczędność czasu [kreatory wprowadzenia, szablony branżowe, programy rejestracji zbiorczej], automatyzację codziennej pracy [samoobsługa przez użytkownika końcowego, mechanizm zgodności, powiadomienia użytkownika końcowego] i uzyskiwane dane analityczne [modułowe pulpity, prekonfigurowane raporty, szczegółowe dzienniki zdarzeń].

Aplikacje i dane firmowe chronione są na wielu poziomach. Bezpieczeństwo w systemach EMM opiera się na ochronie punktu końcowego, umieszczeniu aplikacji w kontenerach, zabezpieczeniu danych oraz ochronie sieci.

Aby zapewnić kompleksową obsługę i ochronę zasobów przedsiębiorstwa, systemy AirWatch firmy VMware można integrować z najlepszymi

rozwiązaniami producentów: aplikacji i platform do ich tworzenia, bezpieczeństwa, tożsamości, a także zawartości.

Dlaczego warto wybrać rozwiązania AirWatch?

- Lider w branży, posiadający udowodnione sukcesy
- Najlepszy w branży zestaw rozwiązań na potrzeby miejsca pracy
- Uniwersalne rozwiązanie o najszerzym środowisku
- Nowoczesna platforma UEM ułatwiająca zarządzanie punktem końcowym
- Wszechstronne usługi edukacyjne i wsparcie globalne

Mobile Device Management MDM na przykładzie iOS

Krajobraz współczesnego miejsca pracy zmienia się dynamicznie. Pracownicy są bardziej mobilni, w dużym stopniu korzystają z aplikacji mobilnych – zarówno służbowo, jak i prywatnie. Współcześni użytkownicy oczekują wolności w sposobie pracy.

W tradycyjnym podejściu, gdzie korzystano jedynie z ręcznej konfiguracji, a dodatkowo wyłączano lub blokowano niektóre funkcjonalności, prywatność

użytkowników była pomijana, a efektywność pracy o wiele niższa, niż w nowym modelu pracy. Nowy model zarządzania jest sprawdzonym sposobem na balans pomiędzy efektywnością pracownika, a jego zadowoleniem z pracy.

Opiera się on na wbudowanej strukturze zarządzania i lekkim podejściu do niego. Ziarnista kontrola pozwala na respektowanie prywatności użytkownika.

W systemie MDM dane prywatne użytkownika są chronione, a dane służbowe są zarządzane.

MDM może widzieć:

- Nazwę urządzenia
- Numer telefonu
- Numer seryjny
- Nazwę i numer modelu
- Pojemność i wolne miejsce
- Wersję iOS
- Zainstalowane aplikacje

MDM nie może zobaczyć:

- Prywatnych maili, kalendarzy i kontaktów
- SMS, czy iMessages
- Historii przeglądarki Safari
- Listy rozmów telefonicznych, czy FaceTime
- Prywatnych notatek, czy przypomnień
- Częstotliwości używania aplikacji
- Lokalizacji urządzenia

Co zyskujemy dzięki MDM?

- Ustawienia
 - Szybkie uruchomienie i konfiguracja
 - Zarządzanie konfiguracjami i aktualizacjami
 - Polityka Kodu Bezpieczeństwa
 - Zarządzanie kontami
 - Klasyfikacja kont zarządzanych
- Restrykcje – mogą dotyczyć funkcjonalności urządzenia, aplikacji, iCloud, bezpieczeństwa i prywatności.
- Zawartość – zarządzanie aplikacjami, możliwością otwarcia w aplikacjach, rozszerzeniami, książkami, domenami, czy klawiaturami.
- Polecenia – istnieją pewne typy poleceń, które zapewniają bezpieczeństwo urządzenia, możliwość zarządzania hasłami oraz wyświetlania przez AirPlay.
- Zapytania – pozwalają na monitorowanie zgodności, zapewniają utrzymanie aplikacji przez użytkownika, umożliwia uruchomienie alarmu, gdy niedozwolona zawartość została dodana.

Apple Device Enrollment Program oraz Apple Volume Purchase Program

Dla użytkowników urządzeń Apple i systemu iOS, AirWatch przygotował specjalne programy:

Apple Device Enrollment Program

Program DEP pozwala na automatyczne zapisanie nowych urządzeń do systemu MDM. W ramach tego programu profile MDM są dodatkowo zabezpieczone przed skasowaniem. Dzięki programowi, możliwe jest ominięcie kroków konfiguracji wstępnej, a pełne nadzorowanie następuje od pierwszej chwili po wyjęciu przez użytkownika urządzenia Apple z pudełka.

Apple Volume Purchase Program

Ten program umożliwia zakupy aplikacji i książek w dużej ilości, oferując kontrolę i zarządzanie własnością na urządzeniach mobilnych. Dzięki programowi VPP istnieje możliwość prostego przekazania zawartości dla użytkowników przy współpracy systemu MDM.

Przetwarzanie danych osobowych na urządzeniach mobilnych – kwestie prawne

Kwestie prawne związane z wykorzystywaniem urządzeń mobilnych do przetwarzania danych osobowych, powinny być omówione indywidualnie z osobami odpowiedzialnymi za bezpieczeństwo w firmie.

Zadania w związku z ustawą, a systemy informatyczne [tablety i smartfony]:

- Ustalenie, czy wymagana jest rejestracja zbioru danych osobowych
- Wydawanie i odbieranie upoważnień do przetwarzania danych osobowych w danym zbiorze, prowadzenie ewidencji wydanych upoważnień
- Zabezpieczenie danych osobowych w systemach informatycznych [EMM mogą stanowić zabezpieczenie danych]
- Zapoznavanie pracowników z przepisami o ochronie danych osobowych [należy poinstruować pracowników również o tym, jak przechowywać dane na urządzeniu mobilnym, z którego korzystają oraz jak chronić samo urządzenie przed nieautoryzowanym dostępem, zgubieniem, czy kradzieżą]
- Usuwanie również z urządzeń mobilnych danych osobowych, które nie są już przetwarzane [należy pamiętać, aby takie dane usunąć ze wszystkich nośników]
- Poddawanie się kontroli Generalnego Inspektora Danych Osobowych [GIODO]

Jak uregulować kwestie smartfonów w organizacji z punktu widzenia wymagań związanych z ochroną danych osobowych?

W polityce bezpieczeństwa danych osobowych powinniśmy uwzględnić urządzenia przenośne

w części dotyczącej obszarów przetwarzania danych osobowych, wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, sposobów przepływu danych między poszczególnymi systemami informatycznymi, środków technicznych i organizacyjnych stosowanych w celu ochrony danych osobowych.

Zmiany należy wprowadzić również do instrukcji zarządzania systemami informatycznymi, służącymi do przetwarzania danych w części dotyczącej: sposobu, miejsca i okresu przechowywania kopii zapasowych, procedury tworzenia kopii zapasowych, środków zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania, procedury wykonywania przeglądów i konserwacji systemów i nośników informacji służących do przetwarzania danych osobowych.

W systemie informatycznym, służącym do przetwarzania danych osobowych, stosuje się mechanizmy kontroli dostępu do danych w przypadku, kiedy dostęp do danych przetwarzanych w systemie posiadają co najmniej dwie osoby. Wtedy w systemie powinien być rejestrowany odrębny identyfikator dla każdego użytkownika, a dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

Należy pamiętać, że identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie. W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana powinna następować nie rzadziej, niż co 30 dni, a samo hasło powinno się składać co najmniej z 6 znaków.

Dane osobowe przetwarzane w systemie informatycznym, zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe

przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, a usuwa się je niezwłocznie po ustaniu ich użyteczności. Osoba użytkująca komputer przenośny, zawierający dane osobowe, powinna zachowywać szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych. Dodatkowo stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

Dobre praktyki do zastosowania przy zarządzaniu urządzeniami mobilnymi w przedsiębiorstwie:

- Zakaz używania urządzeń mobilnych przez osoby inne, niż użytkownicy, którym zostały one powierzone
- Zakaz pozostawiania urządzeń mobilnych bez nadzoru, szczególnie w samochodach, hotelach i innych miejscach publicznych
- Zakaz podłączania urządzeń mobilnych do otwartych sieci internetowych Wi-Fi, tzw. „hot spot”
- Zakaz przechowywania w pamięci urządzenia zbiorów danych osobowych

- Zakaz samodzielnej modernizacji urządzeń mobilnych oraz użytkowanego przez nie oprogramowania
- Instalowanie na urządzeniach mobilnych wyłącznie zaufanych/ sprawdzonych aplikacji mobilnych [instalacja powinna być możliwa wyłącznie po autoryzacji osoby z odpowiednimi uprawnieniami, np.: z działu IT]
- Należy dokonywać aktualizacji: twórcy oprogramowania takiego, jak np.: Android i iOS dokładają ciągłych wysiłków, aby za pomocą aktualizacji, zamknąć luki i potencjalne exploity
- Instalacja systemu umożliwiającego zdalne usunięcie danych oraz poinformowanie użytkowników o tej możliwości w procedurze

Ochrona zasobów przedsiębiorstwa zależy również od zabezpieczeń zaimplementowanych w platformach mobilnych, w których co roku rozwijane są procesy szyfrowania, zabezpieczania, przechowywania i usuwania danych. Świetnym tego przykładem są urządzenia mobilne firmy Apple, które zostały zaprojektowane z myślą o użytkownikach mobilnych i zagrożeniach, na jakie są narażane. Systemy EMM firmy AirWatch wykorzystują API udostępnione przez producentów systemów mobilnych do rozszerzenia możliwości ochrony zasobów o swoje technologie.

Rozwiązania mobilne – oferta Innergo Systems

Nasza oferta rozwiązań mobilnych dla biznesu pozwala na indywidualne dostosowanie usług do potrzeb i możliwości firmy, zapewniając jej kompleksowe wsparcie poprzez dobór odpowiednich usług. W ramach współpracy przeszkolimy personel, przygotujemy systemy i dostarczymy urządzenia.

Wdrożenie rozwiązań mobilnych nie wiąże się z dużym obciążeniem finansowym. Oferujemy różne modele finansowania: leasing lub wynajem długoterminowy. Dzięki temu inwestycja nowego wdrożenia to stała miesięczna opłata – brak konieczności angażowania środków z góry. Dodatkowo zyskuje się usługi wsparcia i serwisu oraz przedłużoną gwarancję aż do 24 miesięcy.

Aby spełnić wszelkie oczekiwania klientów dostarczamy wsparcie dla użytkowników końcowych, dbamy o bezpieczeństwo i pomagamy w zarządzaniu, zapewniamy zastępcze urządzenia już na następny dzień roboczy, a dzięki temu ograniczamy zaangażowanie wewnętrznych zasobów IT.

Rozwiązania mobilne w biznesie to nowy sposób pracy. Progresywne przedsiębiorstwa przekazują swoim pracownikom najlepsze narzędzia, technologie i aplikacje, aby wspierać w rozwoju zawodowym i efektywnej pracy.

Systemy EMM są odpowiedzią na potrzeby dzisiejszego mobilnego świata biznesu, gdzie bezpieczeństwo i funkcjonalność są kluczem do osiągnięcia przewagi nad konkurencją.