techstep

Techstep Essentials MDM

Instrukcja zarządzania systememem

Data: 18/10/2023

Spis treści

OPUBLIKOWANY PRZEZ:

Techstep Poland S.A.

Ul. Wajdeloty 12A

80-437 Gdańsk

1 Opis struktur zbiorów przechowujących dane osobowe

Zbiór serwery obejmuje dane podmiotów dla których zostało założone konto/organizacja w aplikacji Techstep Essentials MDM udostępnionej odpłatnie przez Administratora jego klientom.

Zbiór zawiera dane dostępowe do środowisk produkcyjnych w tym adres serwera, port, login, hasło oraz dodatkowe ustawienia. Są to dane poufne dostępne wyłącznie z sieci wewnętrznej Techstep udostępnione tylko upoważnionym pracownikom firmy. Pobranie i użycie wskazanych danych jest każdorazowo raportowane do systemu z informacją kto i kiedy wystąpił o udostępnienie takich danych.

W ramach zbioru serwery możemy wydzielić następujące podzbiory:

1. serwery dedykowane
2. serwery współdzielone
3. serwery zarządzane przez osoby trzecie / niezależne od Techstep

W przypadku serwerów dedykowanych i współdzielonych dane gromadzone, przechowywane i przetwarzane są w formie elektronicznej, w ramach aplikacji Techstep Essentials MDM, na serwerze VPS należącym do OVH Sp. z o.o. z siedzibą we Wrocławiu (54-402), ul. Szkocka 5 lok. 1, który to serwer OVH Sp. z o.o. odpłatnie udostępnia Administratorowi w ramach świadczonej na jego rzecz usługi.

Dostęp do danych wymaga zalogowania się do aplikacji Techstep Essentials MDM z uprawnieniami administratora przy wykorzystaniu identyfikatora użytkownika oraz hasła i/lub tokenu. Dostęp do serwera, na którym przechowywane są dane, wymaga zalogowania przy wykorzystaniu identyfikatora użytkownika oraz hasła, przy czym samo uzyskanie dostępu do serwera nie pozwala na odczytanie danych osobowych, ponieważ są one zapisane w specjalnej strukturze plików i bazie danych kompatybilnej z aplikacją Techstep Essentials MDM. Odczytanie danych osobowych możliwe jest wyłącznie przy wykorzystaniu aplikacji Techstep Essentials MDM, po zalogowaniu się do niej przy wykorzystaniu identyfikatora użytkownika oraz hasła. Serwer, na którym przechowywane są dane, znajduje się we Francji.

Dane zbierane są bezpośrednio od klientów Administratora i trafiają do zbioru w wyniku założenia dla nich konta użytkownika w aplikacji Techstep Essentials MDM. Dane każdego klienta (użytkownika) przypisane są do założonego dla niego konta. Klient wprowadzający dane zgadzając się na warunki licencji przy pierwszym zalogowaniu oświadcza, iż jest świadomy skutków prawnych związanych z prawidłowym wprowadzeniem danych.

Dane przetwarzane są w celu realizacji umowy o świadczenie usług w zakresie udostępnienia aplikacji Techstep Essentials MDM zawartej przez klienta z Administratorem.

System oparty jest na relacyjnych bazach danych, toteż istnieje nieograniczona możliwość zidentyfikowania użytkownika za pomocą z pozoru nieistotnych danych. Sytuacja taka wymagałby jednak użycia znacznego nakładu czasu i pracy oraz złamania zastosowanych zabezpieczeń lub uzyskania nieuprawnionego dostępu.

System umożliwia nałożenie ograniczeń w dostępie i wprowadzaniu danych poprzez przypisanie odpowiednich, konfigurowalnych ról. W najmniej restrykcyjnym ujęciu system pozwala na wprowadzenie przez Administratora następujących danych:

- w odniesieniu do użytkownika:

Imię, nazwisko, login, hasło (w postaci zaszyfrowanej), Państwo, Firma, dział, stanowisko, telefon do biura, telefon komórkowy, identyfikator, adres e-mail, grupa, rola, certyfikat, nazwa użytkownika IM, Identyfikator użytkownika Lotus Notes, nazwa użytkownika MSexchange, adres e-mail MSexchange, Domenta MSexchange, Hasło msExchange, nazwa użytkownika ShoreTel RoamAnywhere, hasło ShoreTel RoamAnywhere, Directory Number ShoreTel RoamAnywhere, Enterprise Number ShoreTel RoamAnywhere, nazwa użytkownika APN, Hasło APN, nazwa użytkownika EAP, hasło EAP, Realm EAP

- w odniesieniu do urządzenia:

Model, platforma, karta SIM, opis, IMEI, UID, numer seryjny, WLAN MAC, operator komórkowy, typ własności(radio), należy do, zakupiony w, data zakupu, gwarancja do, numer umowy, serwisowany przez, (radio:) brandowany, 3G, bezprzewodowa sieć, wbudowana kamera, na stanie

- w odniesieniu do karty SIM:

*użytkownik, numer telefonu, Państwo, operator komórkowy, IMSI, PIN, PUK, numer seryjny, numer umowy, zakupiona od, data podpisania umowy, data wygaśnięcia umowy, plan taryfowy, (radio:) roaming, rozmowy międzynarodowe, pakiet danych, zastrzeżony numer, typ umowy

- w odniesieniu do organizacji:

Nazwa, Państwo, Domyślny język, Województwo, Miasto, Ulica, kod pocztowy, e-mail, numer telefonu, role,

- własne niestandardowe pola:

System umożliwia stworzenie nieograniczonej liczby własnych pól w odniesieniu do użytkownika, urządzenia, karty sim oraz grupy. Techstep Essentials MDM nie bierze odpowiedzialności za treść, prawidłowość i dodatkowe zabezpieczenie takich danych przy czym pole oznaczone jako hasło jest przez system maskowane. (tekst, liczba, hasło, data, słownik)

- dane automatycznie zbierane przez system:

W zależności od zainstalowanych modułów system może pobierać dodatkowe dane takie jak: lokalizacja urządzenia, treść wiadomości sms, lista odwiedzanych stron www, lista wybieranych i odebranych połączeń itd. wskazane dane odnoszą się do konkretnego urządzenia jednak z uwagi na mnogość dostępnych relacji mógłby zostać wykorzystane do wskazania konkretnego użytkownika

Administrator powierzył przetwarzanie wszystkich danych zawartych w zbiorze spółce OVH Sp. z o.o. z siedzibą we Wrocławiu (54-402), ul. Szkocka 5 lok. 1 w celu świadczenia na rzecz Administratora usługi w postaci udostępniania Administratorowi serwera VPS, na którym przechowywane są dane osobowe.

Dodatkowo/Wyjątkowo w ramach doraźnej pomocy pracownicy Techstep mogą świadczyć usługi wsparcia dla Klientów, u których rozwiązanie zostało zainstalowane w infrastrukturze Klienta, do której Techstep nie posiada nieograniczonego i nienadzorowanego dostępu.

Realizacja pomocy przeprowadzana jest na zasadach określonych przez zgłaszającego incydent podmiotu i na wskazanych przez niego warunkach. Działania wykonywane są w sposób ograniczający pozyskanie jakichkolwiek danych, a wszelkie dane które mógłby zostać przetwarzane objęta są odrębną zgodą na ich pod-powierzenie, dane takie nie są gromadzone.

Wszelka komunikacja między serwerem i urządzeniami jest zaszyfrowana. Techstep Essentials MDM wykorzystuje SEAC (Secure Enrolment and Communication) do komunikacji między serwerem Essentials MDM, a urządzeniami mobilnymi.

2 Opis zastosowanych metod i środków uwierzytelniania

- Użytkownik nie ma możliwości samodzielnego utworzenia konta do systemu Techstep Essentials MDM. Tworzenie konta możliwe jest wyłącznie przez użytkownika z prawami administratora lub super admina.
- Do utworzenia nowego konta niezbędne jest podania loginu użytkownika pozostałe parametry są opcjonalne, jednak logowanie do systemu będzie możliwe wyłącznie po wygenerowaniu hasła (jego zmiana może zostać wymuszona przy pierwszym zalogowaniu), zaznaczeniu opcji "może się logować" oraz określeniu roli tj. zakresu zasobów do jakich użytkownik będzie miał dostęp, bez określenia tych parametrów dostęp do danych będzie miał wyłącznie administrator.
- Konta tworzone przez administratora tworzone są w obrębie konkretnej organizacji. Każde tworzone konto posiada swój unikalny numer ID.
- Użytkownicy, którym przyznano dostęp do podsystemu przetwarzania danych osobowych (w tym identyfikator dostępu do systemu) ustalają hasło dostępu z Administratorem Bezpieczeństwa Informacji.
- Hasło jest informacją o poufnym charakterze i należy zachować je w tajemnicy.
- Obowiązuje ścisły zakaz ujawniania hasła osobom trzecim, w tym innym użytkownikom.
- Hasła do wszystkich podsystemów użytkowanych w Zakładzie/Dziale należy przechowywać w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
- Osobą odpowiedzialną za bezpieczne przechowywanie listy identyfikatorów wraz z hasłami wymienionymi w pkt. 4 jest Administrator Informacji.
- Dostęp do listy identyfikatorów i haseł użytkowników wszystkich podsystemów użytkowanych w Zakładzie/Dziale posiada Administrator Informacji. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie Administratorowi Informacji lub bezpośrednio Administratorowi Bezpieczeństwa Informacji, który ustali nowe hasło.

3 Procedury rozpoczęcia, zawieszenia I zakończenia pracy przeznaczone dla użytkowników systemu

W celu rozpoczęcia pracy z systemem Techstep Essentials MDM, należy zalogować się na stronie https://<nazwa serwera>

1. używając loginu oraz aktualnego i poufnego hasła dostarczonego przez administratora,
2. używając loginu dostarczonego przez administratora oraz aktualnego i poufnego tokenu wygenerowanego przez system otrzymanego na zdefiniowany w bazie numer telefonu poprzez wiadomość sms lub odczytanego z dedykowanej mobilnej aplikacji Techstep Essentials MDM

Użytkownik podczas logowania do systemu Techstep Essentials MDM nie może ujawniać hasła osobom trzecim, w tym innym administratorom oraz pozostawiać zapisanego hasła w pobliżu stanowiska pracy i innych pracowników.

Użytkownik zobligowany jest do skutecznego wylogowania się z systemu Techstep Essentials MDM za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od długości okresu jego nieobecności.

Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj”

Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych.

W przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu, użytkownik niezwłocznie zawiadamia o zaistniałym fakcie Administratora Informacji lub bezpośrednio Administratora Bezpieczeństwa Informacji.

4 Sposób odnotowywania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

Administrator powierzył przetwarzanie wszystkich danych zawartych w zbiorze spółce OVH Sp. z o.o. z siedzibą we Wrocławiu (54-402), ul. Szkocka 5 lok. 1 w celu świadczenia na rzecz Administratora usługi w postaci udostępniania Administratorowi serwera VPS, na którym przechowywane są dane osobowe.

5 Sposób odnotowywania sprzeciwu wobec przetwarzania danych osobowych

Podczas pierwszego zalogowania się użytkownika do usługi Techstep Essentials MDM, przed uzyskaniem dostępu do jakichkolwiek danych wyświetlana jest umowa pomiędzy licencjodawcą a użytkownikiem końcowym, określająca warunki udzielenia licencji na korzystanie z oprogramowania (EULA) informująca o charakterze i zasięgu przetwarzanych danych. Zgoda jest niezbędna dla prawidłowego funkcjonowania usługi, dlatego w przypadku braku jej udzielenia dostęp do danych i funkcjonalności nie zostanie nadany, a fakt ten zostanie odnotowany w bazie danych z następującymi danymi: unikalny numer użytkownika, który nie zgodził się na warunki, unikalny numer instytucji, z której nastąpiło odrzucenie umowy, unikalny numer umowy wskazujący na konkretne ustalenia oraz datę i czas w jakim nastąpiło odrzucenie.

6 Procedury anonimizacji danych osobowych

W przypadku oprogramowania Techstep Essentials MDM z uwagi na charakter usługi oraz relacje między wprowadzonymi danymi w celu zapewnienia prawidłowego funkcjonowania aplikacji anonimizacja danych nie jest możliwa. Brak zgody na powyższe skutkuje brakiem możliwości świadczenia usługi.