Cyberdefence 24

15.07.2021

BLACKBERRY MESSENGER ENTERPRISE – BEZPIECZNE NARZĘDZIE KOMUNIKACJI

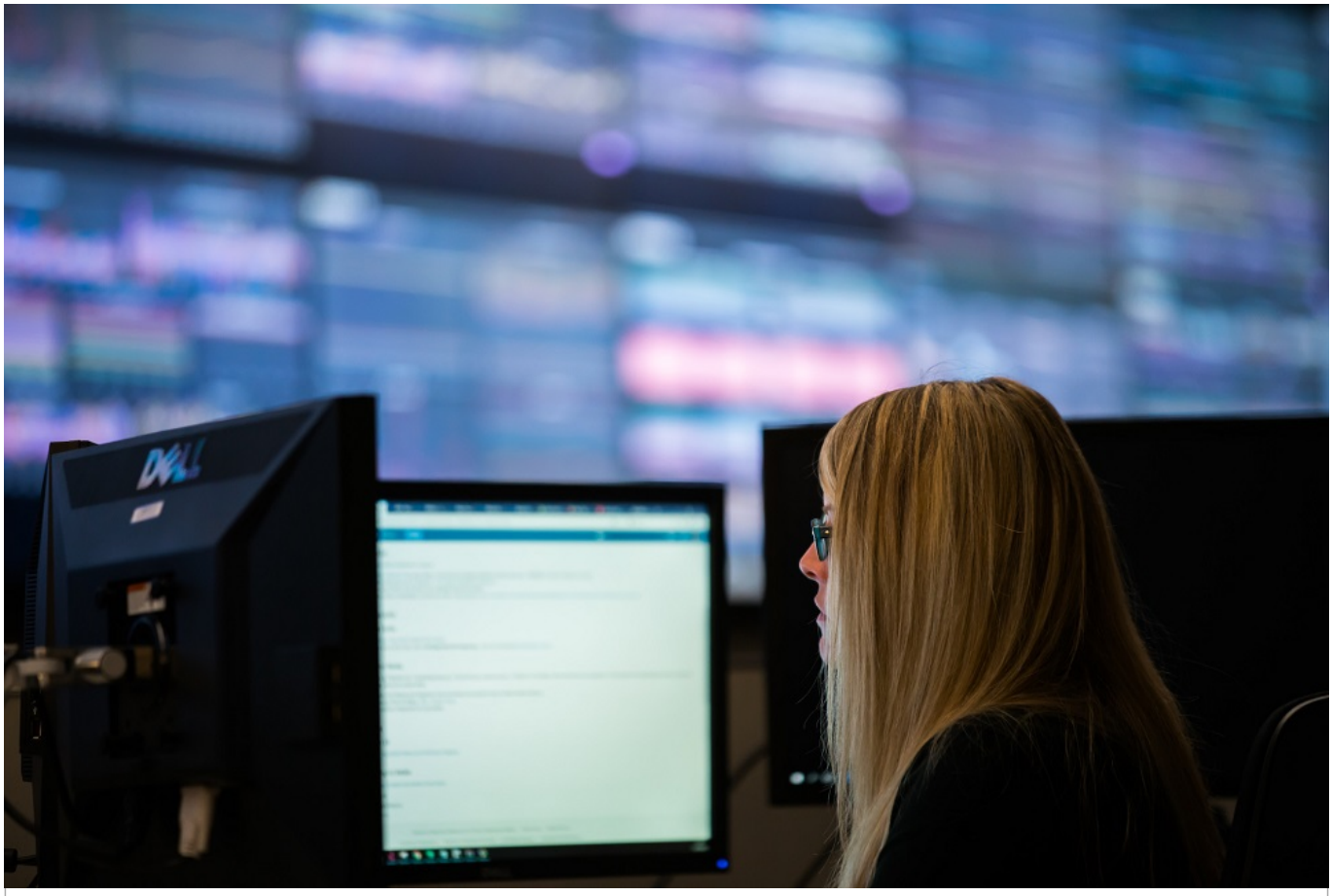
Bezpieczeństwo danych to dziś temat, który odmieniany jest przez wszystkie przypadki. Na ten aspekt szczególną uwagę zwracają specjaliści, którzy często wymieniają między sobą wrażliwe wadomości. Narzędzie BlackBerry Messenger Enterprise zapewnia możliwość wymiany informacji stanowiących tajemnicę słyżbową, a przy tym szybkość, prostotę i zapewnia gwarancję prywatności.

W ostatnich tygodniach opinię publiczną rozgrzewa dyskusja na temat wycieku maili przedstawicieli władzy, bezpieczeństwa danych, obiegu informacji istotnych z punktu widzenia państwa oraz konieczności stosowania odpowiednich zabezpieczeń w przypadku użycia służbowych skrzynek. Przy okazji wycieku z poczty mailowej ministra Michała Dworczyka - wymiany korespondencji między nim, a przedstawicielami rządu - w mediach pojawiły się również informacje o braku zaufania polityków do sejmowej poczty.

W rozmowach z portalem CyberDefence24.pl politycy wskazywali, że częstym powodem użycia prywatnych skrzynek do załatwiania spraw państwowych jest fakt braku zaufania do oferowanych im systemów zabezpieczeń. Co smutne, nie ufają również sobie nawzajem oraz przedstawicielom administracji, dlatego wolą korzystać z narzędzi, których działanie powinno wzbudzać wątpliwości. Wielu posłów przyznało także, że używają nieautoryzowanych komunikatorów, takich jak WhatsApp, Telegram czy Signal, choć nie mają żadnej gwarancji (poza zapewnieniami właścicieli tych platform), że ich dane są bezpieczne.

Co więcej, minister sprawiedliwości i Prokurator Generalny Zbigniew Ziobro stwierdził – odnosząc się do sprawy byłego ministra Sławomira Nowaka – że polskie służby mogły mieć dostęp do treści jego rozmów. „Są inne, nieujawnione przez nas materiały operacyjne, w tym treść rozmów z komunikatorów - WhatsApp i Signal - co do których panowie byli przekonani, że są dla polskich służb nieuchwytne, niedostępne dla polskiej prokuratury. Mylili się i to są bardzo ciekawe rozmowy, które w przyszłości ujawnimy” – zapowiedział.

Szyfrowany czat, wideorozmowa i rozmowy głosowe



Fot. BlackBerry/ materiały prasowe

Warto zatem zastanowić się nad alternatywą dla wskazanych wyżej platform i wybrać mniej oczywistą, ale bezpieczną propozycję – program, który chroni prywatność i dane użytkownika. Taką alternatywą może okazać się BlackBerry Messenger Enterprise, stworzony przez firmę z siedzibą w Kanadzie, kraju członkowskim NATO.

Narzędzie zostało wprost dostosowane do oczekiwań i wymagań przedstawicieli administracji, biznesu, funkcjonariuszy służb oraz osób odpowiedzialnych za zarządzanie kryzysowe, których komunikacja musi być skuteczna i natychmiastowa, ze względu na szczególny charakter ich pracy. Przede wszystkim wyzwaniem jest zapewnienie im 100-procentowej gwarancji bezpieczeństwa w czasie odbywania rozmów głosowych, wideo czy wymieniania wiadomości na czacie.

Nie jest to jednak niemożliwe - w tym przypadku narzędzie zostało przygotowane w ten sposób, aby możliwa była m.in. komunikacja dla informacji wrażliwych bez ryzyka ich przejęcia przez podmioty trzecie, by maksymalnie zminimalizować ryzyko wycieku istotnych informacji, tak jak to się dzieje z innymi platformami czy pocztą e-mail lub by mogło służyć jako alternatywa w razie ataku czy awarii służbowej infrastruktury.

Co w praktyce oznacza korzystanie z BlackBerry Messenger Enterprise? Używanie tego narzędzia możliwe jest w każdym czasie i miejscu; by bezpiecznie spotykać się z rozmówcami – istnieje rozwiązanie natychmiastowego wysyłania swojej lokalizacji w szyfrowanym czacie, a pilne rozmowy mogą odbywać się w formie wideo lub szyfrowanych połączeń telefonicznych. Dodatkową, istotną opcją jest możliwość ustawienia wygaszania każdej pojedynczej wiadomości, która zostanie automatycznie usunięta zaraz po jej przeczytaniu.

Wysłane komunikaty można również przekazywać z jednego zaszyfrowanego czatu do innego, aby zachować płynność w komunikacji między zaangażowanymi w dany proces rozmówcami, a także

cofać, usuwać czy edytować w każdym momencie. Użytkownicy otrzymują także powiadomienie, że ich komunikat został odebrany i odczytany, dzięki czemu mają pewność, że współpracownicy otrzymali wiadomość na czasie. Ma to usprawnić obieg informacji w organizacjach. Możliwe jest także wysyłanie zabezpieczonych notatek głosowych.

By możliwa była organizacja komunikacji w większych zespołach, można szybko tworzyć konferencje wideo oraz czaty, w których weźmie udział do 15 uczestników, bez względu na urządzenie, przebywając zarówno w biurze, jak i poza nim, a zaproszenia generowane są za pomocą linku do szyfrowanego połączenia.

- Dla użytkownika końcowego jest to bardzo intuicyjny interfejs i prostota wysyłania wiadomości, jakie są znane z konsumenckich komunikatorów. Jednocześnie, standard bezpieczeństwa w messengerze Enterprise wykracza poza wytyczne kryptograficzne NIST Suite B. To czyni BBME doskonałym wyborem dla podmiotów rządowych NATO, w tym dla służb mundurowych i wojska. Dla organizacji mowa o pełnej kontroli tego, kto korzysta z platform, zarządzanie grupami, archiwizowanie wiadomości/zgodności, no i oczywiście prywatności danych – komentuje dla CyberDefence24.pl Oleg Orlov, Regional Director – Eastern Europe w BlackBerry.

Korzystanie z narzędzia możliwe jest na wielu urządzeniach bez utraty danych w każdej chwili, a kontakty, które korzystają z BlackBerry Messenger Enterprise można szybko i łatwo pozyskać dzięki zintegrowanej i bezpiecznej chmurze Cloud Directory, a w swojej sieci umieszczać tylko zaufane kontakty.

Zarządzanie systemem jest z kolei bezproblemowe także dla zespołów IT, czuwających nad infrastrukturą w firmach i organizacjach – nie jest konieczne instalowanie nowych aktualizacji systemu operacyjnego czy korzystanie z zewnętrznych serwerów, a uwierzytelnianie czy archiwizowanie wiadomości jest możliwe dzięki BlackBerry® UEM.

Jak chronione są dane?

Bezpieczeństwo użytkowników BBM Enterprise zapewnia szyfrowanie typu end-to-end, stosowane zarówno w czasie użytkowania komunikatora, jak i w trybie offline w systemach Android™, iOS®, BlackBerry® 10, Windows® i macOS.

- Niektóre z cech wyróżniających BBME to np. fakt, że BlackBerry nie wykorzystuje numerów telefonów by oznaczać użytkowników, a także to, że klucze szyfrowania są przechowywane na urządzeniach użytkownika, bez centralnego systemu ich przechowywania utrzymywanego przez BlackBerry. To jedyne rozwiązanie, które posiada taki zdecentralizowany algorytm wymiany kluczy - i BlackBerry wykorzystuje ten patent. To zaawansowana forma negocjowania publicznych kluczy, jednak bez serwera przechowującego klucze w sposób scentralizowany. W konsekwencji, atak w dowolnym punkcie nie poskutkuje ujawnieniem tożsamości użytkowników i kluczy publicznych. Co więcej, w BBMe, każda z wiadomości jest podpisana z przypisaną tożsamością, nie da się jej zmodyfikować, zmanipulować w tranzycie, co rozwiązuje potencjalny problem wynikający z mutowania wiadomości. BlackBerry ma również przewagę konkurencyjną w środowiskach wdrożeń, ze ścisłymi wymogami w zakresie bezpieczeństwa i zgodności, w szczególności w finansach, służbie zdrowia, służbach mundurowych oraz przy użytkowaniu rządowym – mówi nam Oleg Orlov.

Aby mieć pewność, że system odpowiednio chroni przekazywane przez strony informacje, BBM Enterprise wysyła komunikat, że rozmowa jest automatycznie szyfrowana, nawet jeśli odbiorca wiadomości nie jest użytkownikiem komunikatora.

Dwustopniowy system ochrony danych jest zapewniany przez szyfrowanie i odblokowywanie ich przez

klucze symetryczne, które są generowane przez urządzenia ze standardem FIPS 140-2, który poświadcza tym samym, że zachowano odpowiednie normy bezpieczeństwa, skuteczne algorytmy i metody szyfrowania. Natomiast każda wiadomość szyfrowana jest za pomocą nowego, losowego klucza symetrycznego. Drugim stopniem zabezpieczenia ma być protokół TLS, który szyfruje dane przesyłane za pośrednictwem komunikatora oraz sieci, uniemożliwiając osobom postronnym oraz cyberprzestępcom dostęp do przesyłanych informacji, co jest szczególnie istotne w przypadku informacji niejawnych.

Dodatkowe zabezpieczenia to m.in. najwyższe standardy podpisywania, szyfrowania i haszowania; podpis cyfrowy FIPS 186-4, który ma zapewniać autentyczność wiadomości, szyfrowanie symetryczne AES FIPS 197; standard generowania kluczy kryptograficznych NIST SP 800-133 czy standard Secure Hash FIPS 180-4, który zapewnia bezpieczeństwo kodów HMAC, podpisów cyfrowych, wyprowadzania i wymiany kluczy.

To nie wszystko: BBM Enterprise w momencie uruchomienia nowego czatu, tworzy nowy losowy klucz, chroniący metadane oraz wiadomości, które pojawiają się w konwersacji. Wiadomości są szyfrowane wielostopniowo, oprogramowanie używa dwóch typów kluczy kryptograficznych: kluczy tożsamości i kluczy czatu. Wszystkie narzędzia aplikacji zostały skonstruowane tak, by użytkownicy mieli pełną kontrolę nad prowadzoną rozmową, mogli ufać swoim źródłom i być pewnym, kto jest nadawcą wiadomości. Przede wszystkim chodzi również o to, by zawsze mieli potwierdzenie, kiedy ich komunikat dotarł i został odczytany; mogli bezpiecznie dzielić się plikami i notatkami głosowymi oraz by mogli komunikować się w dowolnym czasie, z dowolnego miejsca, w dogodnej lokalizacji.

Gwarancją braku kryzysów i potencjalnego wycieku wrażliwych wiadomości jest bezpieczne narzędzie do wymiany informacji. Zapobiega to przedostaniu się komunikatów w niepowołane ręce, co może zagrażać pozycji nie tylko korporacji, ale – co pokazały ostatnie tygodnie w Polsce – również państwa. Instytucje rządowe muszą być pewne, że do publicznego obiegu nie dostanie się nic, co nie powinno ujrzeć światła dziennego, co ma istotny wpływ na bezpieczeństwo państwa w kontekście współczesnej walki w cyberprzestrzeni. Przyszłość pokaże, że ten, kto jest lepiej zabezpieczony - ostatecznie ma szansę wygrać ten wyścig.

Więcej informacji o tym rozwiązaniu można znaleźć na: www.blackberry.com.

Artykuł powstał we współpracy z firmą BlackBerry.