RAPORT

POKAZ TECHNOLOGII DLA SŁUŻB MUNDUROWYCH "Bezpieczny Komunikator Mobilny"

27 lutego 2020, Warszawa

POLSKA PLATFORMA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Wydarzenie zostało zorganizowane w ramach projektu i-LEAD (www.i-lead.eu), finansowanego przez Komisję Europejską w ramach Programu Horyzont 2020 - program ramowy w zakresie badań naukowych i innowacji, w ramach umowy o dotację numer 740685.

i-LEAD

Wprowadzenie

W dniu 27 lutego 2020 roku w Warszawie Polska Platforma Bezpieczeństwa Wewnętrznego (PPBW) zorganizowała prezentacje dostępnych na rynku bezpiecznych komunikatorów mobilnych.

Szyfrowane komunikatory zapewniają większe bezpieczeństwo i chronią informacje zawarte w przesyłanych przez użytkowników wiadomościach, co jest niezwykle istotne z punktu widzenia właściwego postępowania z informacjami służbowymi, w tym również poufnymi. Celem wydarzenia było zaprezentowanie przedstawicielom różnych służb mundurowych i prokuratury nowych, mniej znanych na polskim rynku rozwiązań do bezpiecznej wymiany wiadomości. W spotkaniu uczestniczyli wyłącznie przedstawiciele służb mundurowych i prokuratury.

Podczas wydarzenia wystąpili:

- **Kamil Kaczyński, Ekspert w zakresie systemów zintegrowanych z mechanizmami kryptograficznymi**

oraz przedstawiciele firm, które dostarczają na rynek najnowsze rozwiązania w tym obszarze:

- **Raw Sp. z o.o.**
- **Evizone Polska Sp. z o.o.**
- **Heinekingmedia GmbH**

Zagrożenia dla użytkowników najpopularniejszych komunikatorów mobilnych

Komunikatory mobilne, takie jak WhatsApp, Viber, Telegram i Signal szturmem zdobyły rzesze użytkowników na całym świecie. Ciężko sobie wyobrazić smartfon, który nie posiada choćby jednego z powyższych. Ich twórcy gwarantują użytkownikom poufność prowadzonej komunikacji poprzez zastosowanie szyfrowania end-to-end dla prowadzonej komunikacji. Gwarancje producentów jak mantrę potwierdzają popularnonaukowe portale traktujące o bezpieczeństwie informacji. W całym tym medialnym szumie brak jest jednak informacji o tym, jak chronione są dane użytkownika przechowywane na jego urządzeniu. Czy baza danych WhatsApp jest szyfrowana? Czy ochrona dostępu z wykorzystaniem kodu PIN w Telegram jest wystarczające? Czy ukryte czaty w Viber rzeczywiście są ukryte? Czy Signal jest remedium na całe zło i stosuje odpowiednie mechanizmy szyfrowania bazy danych? Jak to możliwe, że pomimo braku reklam komunikatory są bezpłatne?

Odpowiedzi na te pytania, przedstawione w prezentacji zostały poparte stosownymi materiałami pobranymi z fizycznych urządzeń z zainstalowanymi aplikacjami. Dodatkowo, przedstawiona została analiza pozyskiwanych przez przykładową usługę komunikatora mobilnego metadanych, jednoznacznie wskazująca, iż brak dostępu do treści prowadzonych rozmów nie jest żadną przeszkodą w profilowaniu użytkowników tego typu aplikacji.

PRELEGENT: KAMIL KACZYŃSKI

Absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej, kierunku Informatyka, o specjalności „Kryptologia". Od 2010 roku zatrudniony na stanowisku asystenta badawczo - dydaktycznego w Instytucie Matematyki i Kryptologii, Wydział Cybernetyki. Od 2011 roku aktywny członek International Association for Cryptologic Research. W toku swojej pracy zawodowej brał udział w realizacji ponad 20 projektów badawczo-rozwojowych, realizowanych na potrzeby obronności państwa, jak i sektora prywatnego. Pełnił role kierownicze, zarządzając wytwarzaniem oprogramowania i rozwiązań kryptograficznych, które zostały z sukcesem skomercjalizowane. Jest autorem i współautorem kilkunastu publikacji naukowych z zakresu kryptologii i steganografii. Aktywny popularyzator idei wykorzystywania systemów gwarantujących bezpieczeństwo informacji.

Autor i współautor licznych algorytmów i rozwiązań kryptograficznych i steganograficznych wyróżnianych na międzynarodowych wystawach wynalazczości. Ekspert w zakresie tworzenia i eksploatacji systemów zapewniających integrację z technologiami blockchain i mechanizmami kryptograficznymi pozwalającymi na zapewnienie poufności, integralności i dostępności danych.

Przedmiotem oferty firmy RAW jest bezpieczna platforma komunikacyjna, która zapewnia bezpieczeństwo i prywatność prowadzonej za jej pośrednictwem komunikacji (aplikacja na smartphona). Wszystkie dane, które przechowuje, są szyfrowane i cała komunikacja jest również szyfrowana bez możliwości przeprowadzenia ataku man-in-the-middle. Komunikator jest równie łatwy w użyciu i oferuje takie same funkcjonalności, jak każda inna, mniej bezpieczna forma komunikacji elektronicznej. Nie przetwarza danych w chmurze, w związku z czym prywatność korespondencji w żadnej mierze nie zależy od intencji dostawcy usługi.

RAW

CYBER & INTELLIGENCE

KOMPLEKSOWA OCHRONA URZĄDZEŃ MOBILNYCH

Komunikator posiada certyfikat bezpieczeństwa NATO do poziomu Restricted. Zarówno aplikacja jak i część serwerowa jest pod całkowitą kontrolą Użytkownika. Konfiguracja serwera nie pozwala w żadnej sytuacji podsłuchać lub zobaczyć treści szyfrowanej komunikacji pomiędzy dwiema aplikacjami uwierzytelnionymi w systemie. Całość platformy zapewnia całkowitą elastyczność działania w postaci tworzenia grup komunikacyjnych, wizualizacji pozycji smartphonów na mapach czy też materiałów audio i video.

RAW to profesjonalny zespół ekspertów zajmujący się tematyką cyberbezpieczeństwa urządzeń mobilnych. Posiadamy własny lab informatyki śledczej. Mamy silne zaplecze kompetencyjne oraz bieżącą praktykę w zakresie cyberbezpieczeństwa smartphonów. Realizujemy Projekt RAW Secure Phone współfinansowany przez NCBiR w ramach którego powstaje bezpieczny telefon wraz z komunikatorem i oprogramowaniem do monitorowania bezpieczeństwa (MTD).

www.rawcyber.pl

EVIZONE

SAFE COMMUNICATIONS NOW

Działalność Evizone Polska jest związana z produkcją software do rozwiazywania problemów związanych z bezpieczną wymianą informacji, zachowaniem zgodności z przepisami gromadzenia, przechowywania i dostępu do danych (corporation compliance (CC)), ochroną bazy wiedzy korporacyjnej i zarządzaniem komunikacją w cyberprzestrzeni. Jednym z produktów Evizone jest bezpieczny komunikator o nazwie: Evizone Secure Messanger (ESM), który jest przeznaczony do bezpiecznej i bezpośredniej komunikacji między pojedynczymi użytkownikami, jak również do wymiany informacji w ramach korporacji.

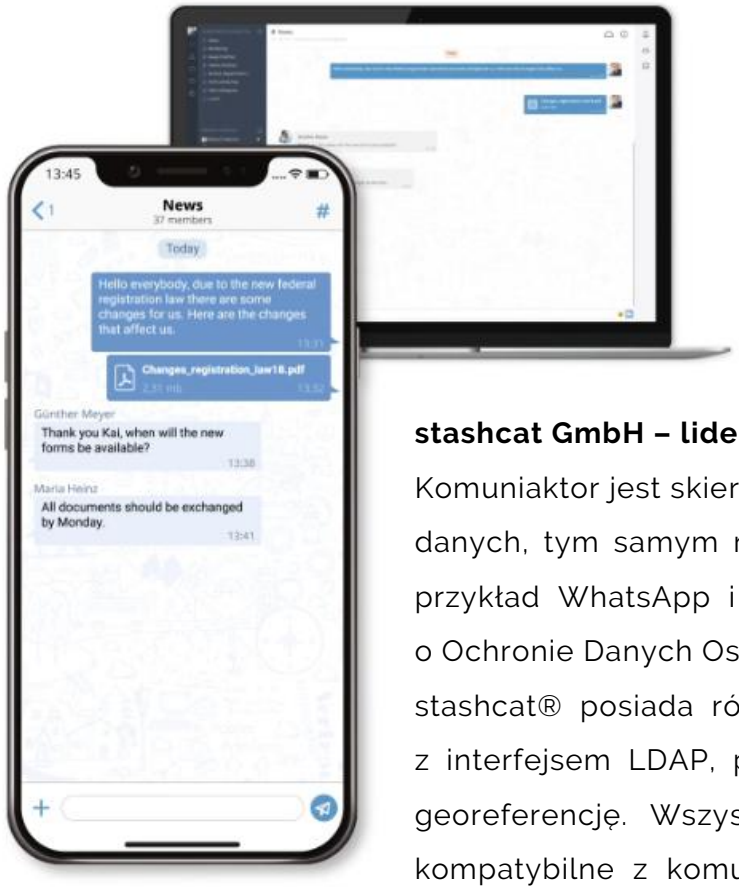
www.evizone.com

ESM zapewnia:

- całkowitą poufność informacji zarówno w komunikacji jeden-do-jednego (podobnie jak w wielu komunikatorach dostępnych na rynku) jak również w komunikacji grupowej,
- poufną komunikację dostępną na każdym urządzaniu,
- możliwość odzyskania komunikacji w razie utraty hasła dzięki kluczowi subskrypcji,
- zarządzanie subskrypcją z poziomu Panelu Subskrypcji bądź przez ActiveDirectory*,
- wieloczynnikową autoryzację z użyciem FreeOTP/Google Auth lub kodów SMS,
- integrację z Mediami Społecznościowymi (autoryzacja przez Google, Facebook itp.),
- możliwość ustalenia cyklu życia informacji,
- możliwość archiwizacji komunikacji w zewnętrznym systemie archiwizacji,
- możliwość integracji ze stroną WWW firmy lub aplikacjami webowymi,
- możliwość brandowania produktu przez dobór: logo, kolorystyki, nazwy i strony logowania.

Bezpieczeństwo ESM jest zapewnione przez:

- wbudowany system PKI – dedykowany Serwer Certyfikatów, który obsługuje wydawanie certyfikatów dla użytkowników systemu, serwera aplikacyjnego SM oraz certyfikatów służących do zabezpieczenia transmisji z dwustronną autoryzacją TLS.
- wiadomości i pliki są szyfrowane za pomocą klucza symetrycznego AES256, a lista dystrybucyjna bazuje na standardzie: PKCS#7.
- certyfikaty i klucze użytkownika, umożliwiające podpisywanie oraz dostęp do zaszyfrowanych wiadomości i stron PDF, są dystrybuowane w formacie: PKCS#12, bez ingerencji użytkownika.
- wszystkie treści, z wyjątkiem metadanych, są przechowywane w systemie, transmitowane w formie zaszyfrowanej i dodatkowo chronione przez dwustronny TLS.



stashcat®

Wysoce bezpieczna współpraca dla biznesu oraz instytucji rządowych!

Bezpieczny, zgodny z rozporządzeniem RODO komunikator z wbudowaną funkcją przechowywania plików, kalendarzem oraz programem do tworzenia ankiet.

stashcat GmbH – lider na rynku bezpiecznych komunikatorów.

Komuniaktor jest skierowany zarówno do biznesu, jak i władz państwowych. Zapewnia poufną komunikację i wymianę danych, tym samym rozwiązanie łączy w sobie funkcjonalności znanych komunikatorów i aplikacji w chmurze, na przykład WhatsApp i Dropbox. Dane zapisane są na niemieckim serwerze danych w zgodzie z Federalną Ustawą o Ochronie Danych Osobowych (Niemcy) lub ewentualnie na serwerach w siedzibie firmy Stashcat.

stashcat® posiada również inne funkcje, takie jak niezależna od numeru telefonu komórkowego baza kontaktów z interfejsem LDAP, prawdziwe szyfrowanie na całej drodze przesyłu danych (eng. end-to-end encryption) oraz georeferencję. Wszystkie przenośne i stacjonarne urządzenia (komputer stacjonarny PC, MAC, Notebook) są kompatybilne z komunikatorem. Ponadto stashcat® może być również obsługiwany i oznaczony jako aplikacja własna.

Gwarantowana poufność danych, możliwość wysyłania opisów osób za pomocą zdjęć, bezpośrednia komunikacja za pośrednictwem kanałów podczas dużych incydentów, czy też łatwość i duża precyzja z jaką można wysyłać lokalizacje to tylko niektóre z zalet, z których niemieckie służby korzystają z wielkim entuzjazmem. W odpowiedzi na powtarzające się prośby, umożliwione zostało również korzystanie z prywatnego urządzenia docelowego, przy jednoczesnym zachowaniu ochrony danych.

stashcat® spełnia wszystkie prawne i merytoryczne wymagania w zakresie ochrony i bezpieczeństwa danych.

Zarejestruj się bezpłatnie, aby uzyskać dostęp do stashcat®.

na stronie: www.stashcat.com/en lub skontaktuj się bezpośrednio z::

Jan Bonde Hennies, tel. +49 (0) 162 416 47 73

email: j.hennies@heinekingmedia.de

www.stashcat.com

Najważniejsze funkcjonalności w skrócie:

Indywidualne czaty | Wymiana rozmów poprzez indywidualne lub grupowe czaty. Treść rozmów i pliki zawsze pozostają w bezpiecznym systemie. Twoje rozmowy odbywają się w przestrzeni, która jest niedostępna dla innych. Poprzez stashcat® masz szansę na szybką komunikację z innymi.

Wewnętrzny katalog | W oparciu o bazę użytkowników firmy, tworzony jest katalog o braku możliwości stałego dostępu do numerów telefonów komórkowych lub ich przenoszenia. Jeśli jest to możliwe, podmiot może być również podłączony do istniejącego protokołu LDAP lub bazy Active Directory. Wszystkie konta użytkowników są aktualizowane i wyświetlane regularnie w katalogu.

Kanały | Funkcja ta pozwala na tworzenie własnych kanałów dla każdego obszaru działalności. Kanały są oznaczone rombem i można je znaleźć za pomocą funkcji wyszukiwania. Funkcja pozwala na łatwą komunikację z grupami lub zespołami.

Szyfrowanie | Szpiegostwo gospodarcze, sabotaż i kradzieże danych należy traktować poważnie, ale niestety są one często bagatelizowane. Dlatego właśnie osobistą misją stashcat® jest zapewnienie zgodnego z zasadami ochrony danych, bezpiecznego i stabilnego rozwiązania komunikacyjnego. Dane firmy i dokumenty są przesyłane w formie całkowicie zaszyfrowanej i znajdują się na zaszyfrowanych serwerach.

Przechowywanie plików | W stashcat® każdy użytkownik otrzymuje indywidualną pamięć, na której pliki mogą być przechowywane, co umożliwia pobieranie oraz wykorzystywanie ich w dowolnym momencie. Zatem każdy użytkownik ma swoje pliki zawsze dostępne na każdym podłączonym urządzeniu i może je udostępniać na żądanie innym użytkownikom lub nawet udostępniać linki zewnętrzne osobom trzecim. Nie tylko każdy użytkownik, ale także kanały oraz rozmowy mają swoje indywidualne miejsce przechowywania plików, w którym można znaleźć pliki bezpośrednio za pomocą funkcji wyszukiwania.

Ankieta | Moduł umożliwia znalezienie terminów spotkań lub przeprowadzenie ewaluacji i drobnych ankiet. Użytkownicy są bezpośrednio powiadamiani o utworzeniu ankiety, a jej wyniki mogą być następnie eksportowane do pliku PDF.

Kalendarz | Organizacja spotkań za pomocą modułu kalendarzowego może być elastycznie wykorzystywana. Poza spotkaniami publicznymi i prywatnymi, można je również udostępniać na kanale. Moduł wspiera codzienną pracę dzięki takim funkcjom, jak możliwość przyjmowania i odrzucania zapytań, synchronizacja z lokalnym kalendarzem urządzenia oraz system filtrów ułatwiający koordynację spotkań, co umożliwia przegląd zbliżających się spotkań.

stashcat®

Polska Platforma Bezpieczeństwa Wewnętrznego

Polska Platforma Bezpieczeństwa Wewnętrznego (PPBW) została powołana w 2005 roku jako miejsce dialogu pomiędzy użytkownikami końcowymi, światem naukowo-badawczym i administracją odpowiedzialną za finansowanie badań. Z czasem PPBW stała się także platformą do budowania konsorcjów naukowo-przemysłowych realizujących działania na rzecz tworzenia dedykowanych rozwiązań technologicznych, wspomagających działania podmiotów odpowiedzialnych za bezpieczeństwo publiczne.

POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

BIURO PPBW:

tel.: +48 61 663 02 21

e-mail: sekretariat@ppbw.pl

www.ppbw.pl

PPBW organizuje wydarzenia, podczas których przedstawiciele służb mundurowych mają możliwość poznać nie tylko rozwiązania dostępne na rynku, ale także wyniki prac badawczo-rozwojowych, prowadzonych w obszarze bezpieczeństwa. Przykłady takich wydarzeń to:

- CP.1 - Technologie - raport dostępny **tutaj**
- I-lEAD Industry Days - raport dostępny **tutaj**

Jeśli jesteś przedstawicielem służb mundurowych zainteresowanym udziałem w tego rodzaju wydarzeniach oraz zauważasz potrzebę organizacji wydarzeń poświęconym poszczególnym tematom - **skontaktuj się z nami!**

Wydarzenie zostało zorganizowane w ramach projektu i-LEAD finansowanego przez Komisję Europejską w ramach Programu Horyzont 2020 - program ramowy w zakresie badań naukowych i innowacji, w ramach umowy o dotację numer 740685.

Celem projektu jest zbudowanie efektywnie działającej sieci służb mundurowych w obszarze: nowych technologii, rozwiązań prawnych, szkoleń i procesów oraz umożliwienie dialogu ze światem nauki i biznesem.

Wiećej informacji nt. projektu znajduję się na stronie: **www.i-lead.eu**

i-LEAD