REPORT

TECHNOLOGY EVENT FOR LAW ENFORCEMENT AGENCIES "Secure mobile messenger"

27 February 2020, Warsaw

POLISH PLATFORM
FOR HOMELAND SECURITY

The event was organized as part of the i-LEAD project (www.i-lead.eu), funded by the European Commission under the Horizon 2020 Framework Program for Research and Innovation, under grant agreement number 740685.

Introduction

On 27 February 2020 in Warsaw, the Polish Platform for Homeland Security (PPHS) organized presentations of secure mobile messengers available on the market.

Encrypted messengers provide greater security and protection of information sent by users, which is essential from the point of view of proper handling of business information, including confidential information. The objective of the event was to present new, less well-known solutions for secure messaging on the Polish market. Only representatives of the LEAs and the prosecutor's office participated in the meeting.

During the event we hosted:

- **Kamil Kaczyński, Expert on systems integrated with cryptographic mechanisms**

as well as representatives of companies which provide the latest solutions in this field in the market:

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

Threats posed by the most popular mobile communicator to its users

Mobile communicators such as WhatsApp, Viber, Telegram and Signal have taken the world by storm. It's difficult to imagine a smartphone that doesn't even have one of those installed. Their creators guarantee users the confidentiality of their conversations by using end-to-end encryption for the communication. Popular science portals dealing with information security regurgitate the manufacturer's guarantees, however, in all this media noise, there is no information about how the user's data stored on a device is protected. Is the WhatsApp database encrypted? Is PIN access protection in Telegram sufficient? Are hidden chats in Viber really hidden? Is Signal a cure-all and uses appropriate database encryption mechanisms? How is it possible that despite the lack of advertising, instant messengers are free of charge?

The answers to these questions given in a presentation were supported by appropriate evidence extracted from physical devices with installed applications. In addition, an analysis of the metadata obtained by a sample mobile communicator service was presented. This analysis clearly indicates that the lack of access to the content of conversations is not an obstacle in profiling users of this type of applications.

SPEAKER: KAMIL KACZYŃSKI

A graduate of the Faculty of Cybernetics of the Military University of Technology, majoring in Computer Science, with the specialization of "Cryptology". Since 2010, he has been employed as a research and teaching assistant at the Institute of Mathematics and Cryptology, Faculty of Cybernetics. Since 2011-an active member of the International Association for Cryptologic Research. In the course of his professional work, he participated in the implementation of more than 20 research and development projects, carried out for the needs of state defense as well as the private sector. He held a managerial position, managing the production of software and cryptographic solutions which were successfully commercialized. He is the author and co-author of several scientific publications on cryptology and steganography. He actively promote the idea of using the systems which guarantee information security.

Author and co-author of numerous cryptographic and steganographic algorithms and solutions awarded at international invention exhibitions. An expert at creating and operating systems ensuring integration with blockchain technologies and cryptographic mechanisms allowing to ensure confidentiality, integrity and availability of data.

RAW

CYBER & INTELLIGENCE

COMPREHENSIVE PROTECTION DEVICES MOBILE

The subject of the offer is a secure communication platform (smartphone application), which ensures security and privacy of the conversations. All stored data as well as all conversations are encrypted without the possibility of man-in-the-middle attack. The communicator is as easy to use and as functional as any other less secure form of electronic communication. It does not process data in the cloud, so the privacy of the correspondence does not depend on the intentions of the service provider.

The communicator has a certificate NATO security to the Restricted level. Not only the application but also the server part is under the total control of the user. The configuration of the server does not allow in any situation to eavesdrop or see the content of the encrypted communication between two applications authenticated in the system. The possibility of creating group conversations, visualizing the position of smartphones on maps or playing audio and video materials makes the whole platform very flexible.

RAW is a professional team of experts dealing with the subject of cyber security of mobile devices. We own a computer forensics lab. We have a strong competence base and current expertise in the field of cyber security. We are implementing The RAW Secure Phone Project co-financed by NCBiR, which involves the creation of a secure phone with a communicator and security monitoring software (MTD).

www.rawcyber.pl

EVIZONE

SAFE COMMUNICATIONS NOW

The activity of Evizone Poland is related to the development of software which solves problems related to secure information exchange, comply with the regulations of data collection, storage and access (corporation compliance (CC)), protection of corporate knowledge base and management of communication in cyberspace. One of the Evizone products is a secure communicator called Evizone Secure Messanger (ESM), which is designed for secure and direct communication between individual users as well as for information exchange within a corporation.

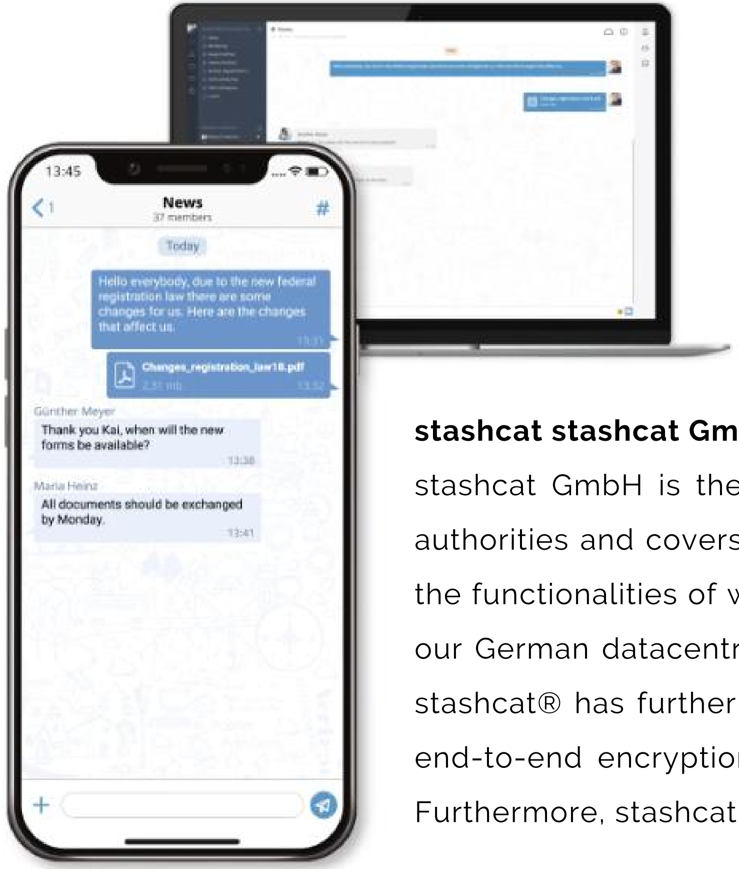
www.evizone.com

ESM provides:

- total confidentiality of information both in one-to-one communication (as in many communicators available on the market) and in group communication,
- confidential communication available on every device,
- the ability to recover communication in case of loss of the password thanks to the subscription key,
- managing your subscription from the Subscription Panel or through ActiveDirectory*,
- multi-factor authentication using FreeOTP/Google Auth or SMS codes,
- integration with social media (authorization by Google, Facebook etc.),
- possibility to determine the life cycle of information,
- possibility to archive communication in an external archiving system,
- possibility of integration with the company's website or web applications,
- possibility to brand the product by selecting: logo, colors, name and login website.

ESM security is ensured by:

- built-in PKI system - special Certificate Server, which supports issuing of certificates for system users, SM application server and certificates for securing transmission with two-way TLS authorization,
- messages and files which are encrypted with the AES256 symmetric key and the distribution list which is based on the standard PKCS#7,
- ·the certificates and user keys, enabling signing and access to encrypted messages and PDF websites, which are distributed in PKCS#12 format, without user intervention,
- all content, except for metadata, is stored in the system, transmitted in encrypted form and additionally protected by bilateral TLS.



13:45

News
37 members

Today

Hello everybody, due to the new federal registration law there are some changes for us. Here are the changes that affect us.
13:31

Changes_registration_law18.pdf
2.31 mb
13:32

Günther Meyer
Thank you Kai, when will the new forms be available?
13:38

Maria Heinz
All documents should be exchanged by Monday.
13:41

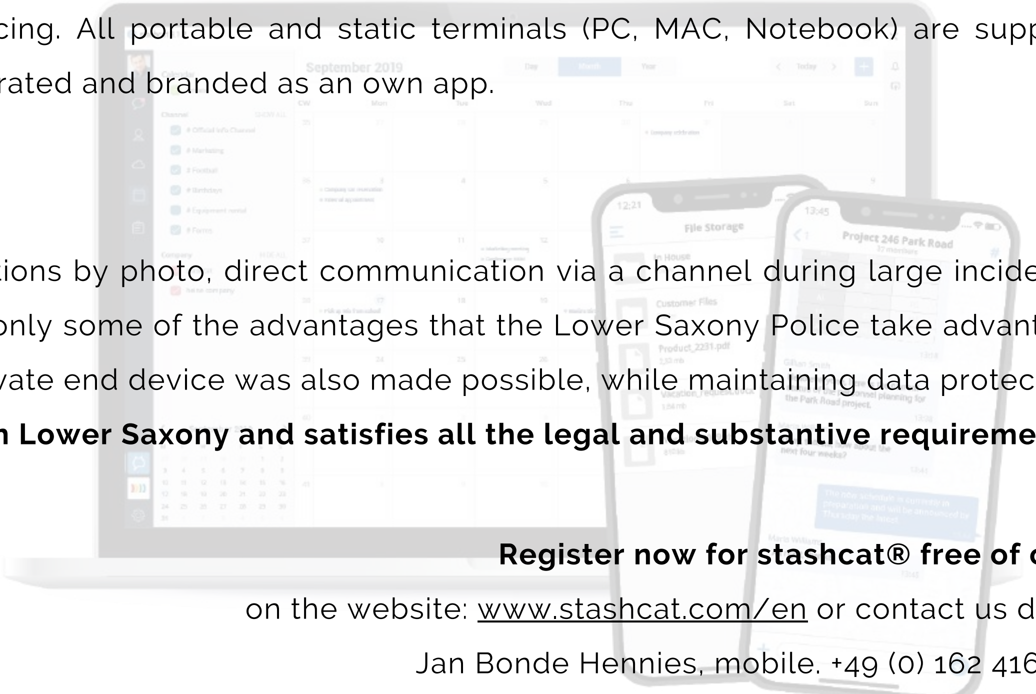
stashcat®

High secure team collaboration for business and government!

GDPR-compliant High Secure Messenger with integrated file storage, calendar and survey tool

stashcat stashcat GmbH – high secure messaging made in Germany!

stashcat GmbH is the market leader for highsecure messaging. It is addressed to corporations as well as public authorities and covers the need for confidential communication and data exchange. Thereby, our solution combines the functionalities of well-known messengers and cloud applications, for instance WhatsApp and Dropbox. Hosted in our German datacentre in accordance with the Federal Data Protection Act (Germany) or alternatively on premise. stashcat® has further features such as a mobile number independent contact database with LDAP interface, a real end-to-end encryption and georeferencing. All portable and static terminals (PC, MAC, Notebook) are supported. Furthermore, stashcat® can also be operated and branded as an own app.



stashcat® in Action: Lower Saxony Police Department

Guaranteed data sovereignty, the possibility to send person descriptions by photo, direct communication via a channel during large incidents, or the ease and great precision with which one can send locations are only some of the advantages that the Lower Saxony Police take advantage of with great enthusiasm. In response to repeated requests, use of a private end device was also made possible, while maintaining data protection. **stashcat® has proven to be a safe base technology for the police in Lower Saxony and satisfies all the legal and substantive requirements for data protection and data security.**

Register now for stashcat® free of charge

on the website: www.stashcat.com/en or contact us directly:

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

email: j.hennies@heinekingmedia.de

www.stashcat.com

The most important features at a glance:

Single Chats | Exchange conversations with one another through single or group chats. Your conversation content and files always stay in a secure environment. Your conversations take place in a setting that is inaccessible to others. In addition to #Channels, you have another opportunity to communicate with colleagues quickly and easily via stashcat®!

Internal directory | Based on the user base of your company, a directory is created - no constant availability or transfer of mobile phone numbers. If available, your organization can also be connected to an existing LDAP or Active Directory. All user accounts are displayed regularly updated in the directory.

Channels | The #Channel feature allows you to create your own channels for each area of your business. #Channels are indicated with a rhombus and can be found via the search function. The #Channel feature allows you to easily communicate with groups or teams.

Encryption | Economic espionage, sabotage and data theft have to be taken serious, but sadly they are seen as underestimate danger of our everyday life. That's why stashcat®'s personal mission is to provide you with a data protection compliant, secure and stable communications solution. Your data and documents are transmitted end-to-end encrypted on encrypted servers across all transmission paths.

Calendar | The organization of appointments via the calendar module can be used flexibly. In addition to public and private appointments, appointments can also be shared in the channel. The module supports your daily routine with features such as the ability to accept and reject inquiries, the synchronization with the local calendar of your device and a filter system for an easy coordination of your appointments. This provides you with an overview of upcoming meetings, customer appointments or corporate events.

File storage | At stashcat®, each user receives their own file storage in which files can be stored, retrieved and used at any time. So each user has his files always available on each connected device and can share them on request with other users or even share external links with non-members. Not only every user, but also #Channels and conversations have their own file storage in which you can find and use stored files directly via the search function.

Survey | The module makes it possible to find appointments for meetings or to conduct evaluations and small surveys. The appointment inquiry as well as the question-and-answer survey can be individually integrated into the daily work routine. Users are notified directly about the creation and the results can then be exported in a PDF file.

stashcat®

Polish Platform for Homeland Security

The Polish Platform for Homeland Security (PPHS) was established in 2005 as a forum for dialog between the end users, the research and development organizations, and the administration responsible for financing of research. With time, the PPHS has also become a platform for formation of scientific and industrial consortia with the aim to develop dedicated technological solutions to support the operations of entities responsible for public security.

PPHS organizes events during which representatives of Law Enforcement Agencies have the opportunity to get to know not only solutions available on the market, but also the results of research and development works carried out in the area of security. Examples of such events are:

- CP.1 - Technologies - report available **hier**
- I-lEAD Industry Days - report abailable **hier**

If you are a representative of LEAs interested in participating in such events and you notice the need to organize events focusing on particular topics – contact us!

POLISH PLATFORM
FOR HOMELAND SECURITY

PPHS OFFICE:

phone: +48 61 663 02 21
e-mail: sekretariat@ppbw.pl

www.ppbw.pl/en

The event was organized as part of the i-LEAD project funded by the European Commission under the Horizon 2020 Framework Program for Research and Innovation, under grant agreement number 740685.

The goal of the project is to build an effective network of LEAs in the area of: new technologies, legal solutions, training and processes, and to enable dialogue with the world of science and business.

More information about the project can be found at: **www.i-lead.eu**

i-LEAD