Sichere Behördenkommunikation:

Die Katze im Sack lassen

Während Institutionen sich mit sicheren Kommunikationswegen schwertun – man denke an die unendliche Geschichte des digitalen Polizeifunks –, schaffen junge Internet-Startups Fakten. Weil WhatsApp und Co. für die behördliche Kommunikation viel zu unsicher sind, macht ein neuer Dienst aus Hannover die Sache jetzt abhörsicher und damit „amtlich“.

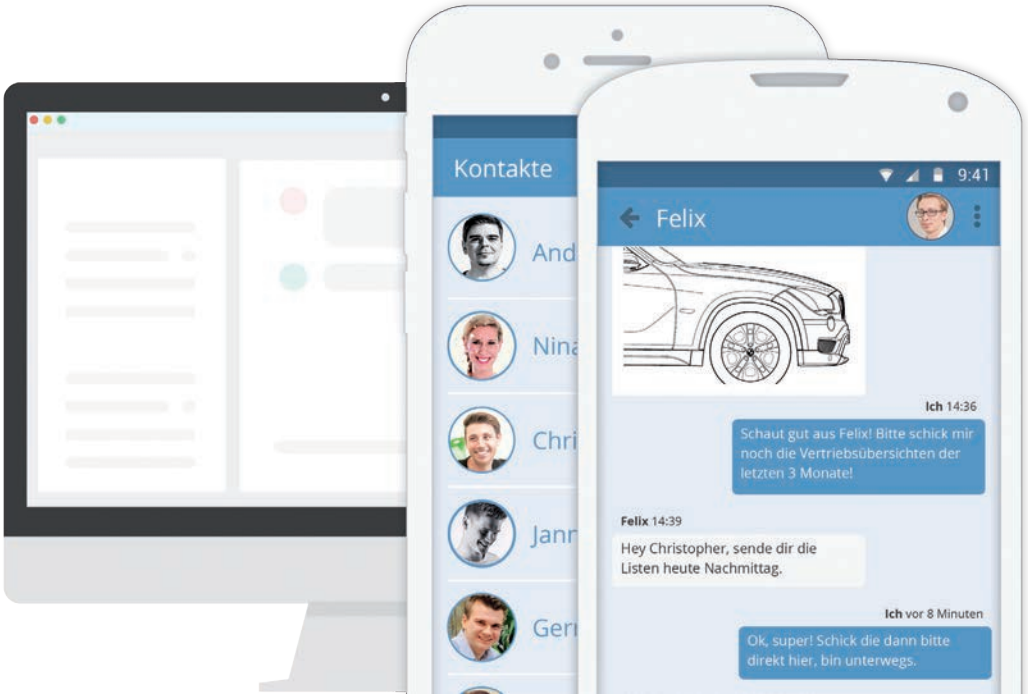
Fast jeder Smartphone-Nutzer hat sich im Privaten an die Annehmlichkeiten der Messenger-Dienste gewöhnt. Allen Sicherheitsbekundungen der meist amerikanischen Unternehmen zum Trotz bezweifelt ein junger deutscher Unternehmer aber, dass die Dienste sicher genug für Firmen- und Behördenkommunikation sind. Es wäre schließlich fatal, wenn zum Beispiel Fahndungsfotos der Polizei, vertrauliche Unterlagen von Ministerien oder Zeichnungen des neuesten Motoren-Prototyps in die falschen Hände gelangten.

Dabei ist gerade im behördlichen Umfeld ein sicherer Umgang mit Daten von zentraler Bedeutung, zumal die Nutzung von WhatsApp oder ähnlichen Diensten im beruflichen Kontext illegal sein kann. Jeder, der zum Beispiel WhatsApp nutzt, stimmt automatisch zu, dass das US-Unternehmen auf die Daten aller Kontakte auf dem Smartphone zugreifen kann. Dies kann erhebliche strafrechtliche Konsequenzen nach sich ziehen, denn nach EU-Datenschutzrecht darf genau das eigentlich nicht sein. Zwar unterliegt die rein private Nutzung des umstrittenen Dienstes nicht dem Bundesdatenschutzgesetz. Menschen, die ihr Smartphone aber beruflich und privat nutzen, können dennoch Probleme bekommen, weil in diesem Fall das Datenschutzrecht sehr wohl greift.

Bislang mangelt es also an einer technisch und rechtlich sicheren Umgebung, in der einerseits Daten sicher abgelegt und Informationen ausgetauscht werden, das Unternehmen oder die Behörde aber nicht verlassen können.

So könnte die Anwendung von Stashcat bei der Polizei aussehen: Fahndungsstände werden von den Kollegen im Außeneinsatz direkt in die Zentrale gemeldet.

Andreas Noack, Geschäftsführer des Kommunikationsunternehmens heinekingmedia aus Hannover, sagt: „Nutzer können bei einem US-Anbieter wie WhatsApp nie ganz sicher sein, dass ihre Daten auch wirklich verschlüsselt werden.“ Das sei nur möglich, wenn die Kunden den Messenger selbst betrie-



ben. heinekingmedia, das zur MADSACK Mediengruppe gehört, hat mit „Stashcat“ gerade einen Messenger auf den Markt gebracht, der sich an Unternehmen und Behörden richtet und die Funktionen von WhatsApp und Dropbox zu einer abhörsicheren Alternative kombiniert.

Das Unternehmen war bislang vor allem als Anbieter digitaler Schwarzer Bretter für Schulen und Firmen bekannt geworden. Stashcat, frei übersetzt in etwa „Geheimversteck-Katze“, richtet sich damit gezielt an Unternehmen und Behörden. Der Messenger-Dienst ist optisch dem großen Konkurrenten WhatsApp nachempfunden, jedoch in Blau gehalten. Technisch nutzt Stashcat aber deutlich mehr Funktionen.

Datenschutzkonforme Plattform

Ob für die Kommunikation im Finanzamt, der Arbeitsagentur oder im Rathaus – Stashcat soll Behörden die Möglichkeit bieten, unkompliziert über angelegte Gruppen miteinander Informationen oder Dokumente auszutauschen. So können beispielsweise in der Gruppe „Standesamt“ alle Mitarbeiter dieser Abteilung miteinander kommunizieren. Raumbelegungspläne für Trauungen können hochgeladen und von allen Gruppenteilnehmern eingesehen werden. Im Einzelchat können einzelne Mitarbeiter in den Austausch treten.

Auch für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) soll Stashcat die Kommunikationslösung für kritische Einsatzsituationen bei Polizei, Feuerwehr oder Rettungsdienst werden. Mit Ende-zu-Ende-Verschlüsselung der Inhalte können so zum Beispiel Fahndungen oder Neuigkeiten einzelner Bezirke über das digitale Schwarze Brett zentral in die Leitstelle kommuniziert werden.

Bei den Funktionen erinnert Stashcat auf dem ersten Blick also ebenfalls an WhatsApp. Allerdings bietet der Messenger noch mehr: Es gibt Einzelchats, Gruppendiskussionen und die Möglichkeit, Themenkanäle anzulegen. Beim Datenaustausch können die Nutzer aber auch Excel- und Powerpoint-Dateien hin- und herschicken. Außerdem steht eine Suchfunktion zur Verfügung. Der Messenger synchronisiert zudem alle genutzten Geräte der einzelnen Nutzer, sodass der Dienst auf allen Plattformen aktuell bleibt. Dazu wird ein Cloudspeicher genutzt.

Vorteile für Behörden

Als wichtigsten Unterschied zu anderen Messenger-Diensten betonen die Macher, dass Stashcat auf Kundenwunsch komplett auf den behörden- oder firmeneigenen Servern laufen kann. „Damit ist die Software grundsätzlich schon deutlich sicherer vor fremden Zugriffen als bei Diensten, die Server Dritter nutzen. Zusätzlich ist Stashcat stark verschlüsselt. Das Einbetten in die Firmeninfrastruktur erlaubt es, den Messenger nach außen gezielt abzuschotten und zugleich Angriffen im Mobilfunknetz oder Internet durch Verschlüsselung entgegenzutreten“, sagt Andreas Noack. Auf Wunsch lasse sich der Messenger sogar der jeweiligen Corporate Identity anpassen. Nutzer könnten den Messenger sowohl auf Computern als auch als App auf Mobilgeräten nutzen.

stashcat

Weitere Vorteile seien übergreifende Kommunikation durch zentrale Kanäle und umgehende Erreichbarkeit, die verzweigte Organisierbarkeit verschiedener Nutzergruppen sowie der einfache Austausch von Dokumenten, Bildern oder Videos über alle Endgeräte und Plattformen. Auch der Aufbau behördenübergreifender Kommunikationsnetzwerke soll mit Stashcat möglich sein. Damit greift der Messenger nicht nur die typischen Funktionen bekannter kommerzieller Dienste auf, sondern erweitert sie für das tägliche Arbeiten im institutionellen Bereich erheblich.

Dass Stashcat anders ist als herkömmliche Messenger, zeigt sich auch darin, dass Privatleute die App zwar in den Appstores der großen Anbieter herunterladen können, für die Benutzung aber eine Registrierung über die firmeneigene Homepage www.stashcat.com benötigen. So kann gar nicht erst der Verdacht aufkommen, dass auch Benutzergruppen, die eigentlich ausgesperrt werden sollen, in den Genuss hoher Abhörsicherheit kommen: „Stashcat ist eine Unternehmenslösung, die nicht frei im Netz geladen und verwendet werden kann. Mit jedem Unternehmen schließen wir einen Vertrag zur Auftragsdatenverarbeitung ab. Selbstverständlich machen wir Gruppen mit kriminellen Absichten nicht zu unseren Kunden“, versichert Noack, auf dessen Stashcat-Homepage derzeit die Möglichkeit besteht, erste Demo-Accounts zu beantragen.

Erste Institutionen haben bereits Interesse an dem System bekundet, deren Namen heinekingmedia aus Datenschutzgründen allerdings nicht nennen darf.

br