Sichere Messenger für Polizisten

Von Prof. Dr. Peter Löbbecke

Nach dem Hochwasser 2013, bei dem die Polizistinnen und Polizisten vieler Bundesländer im Dauereinsatz waren, schrieb ich über die dienstliche Nutzung von WhatsApp (WA), und regte ein Engagement der Polizei in den sozialen Netzwerken an. Später habe ich gefordert, dass die Polizei dringend ein „Organisationswissen" über dieses relativ neue soziale Phänomen aufbauen sollte.

Heute würde ich nicht mehr so schreiben. Man weiß jetzt, in welchem Maße Daten im Internet gesammelt werden – die Nachrichten berichten täglich darüber. Gerade der Messenger-Dienst WA und seine Mutterfirma Facebook (FB) sind dafür bekannt, sogar die Internet-Aktivitäten von Menschen zu sammeln und auszuwerten, die seine Dienste gar nicht nutzen. Sie können insbesondere Personen mit Sicherheitsaufgaben nicht mehr ernsthaft empfohlen werden. Doch Polizisten die Nutzung von WA, FB et cetera verbieten? Sinnvoller wäre es, Alternativen zu suchen und sie den Bediensteten verfügbar machen.

Datenkraken

Die großen Internet-Firmen wie Google, FB/WA und andere bieten ihre Dienste meist kostenlos an, gehören aber zu den Firmen mit dem höchsten (Börsen-)Wert. Ihre Einnahmen stammen aus dem Verkauf von gezielt aufbereiteten Nutzerdaten zu Werbezwecken.

Dazu werden viel mehr Informationen herangezogen, als den meisten Nutzern bewusst ist. Zuerst sind da die Daten, die man in Profilen selbst angibt: Die Freundesliste, Fotos, Gruppenaktivitäten werden ausgewertet. „Private Unterhaltungen" werden zum Teil im Klartext gespeichert – und von großen Rechnern analysiert. Nutzt man WA, kommt das Kontakteverzeichnis des Smartphones mit allen Daten hinzu – wozu übrigens die Erlaubnis jedes Kontaktes nötig wäre!

Sehr viele Webseiten im Internet nutzen Programmcodes, sogenannte Cookies und Tracker, die die Aktivitäten der Besucher ohne deren Wissen aufzeichnen. Diese werden an FB, Google und andere in der Öffentlichkeit kaum bekannte Firmen weitergeleitet, die alle von der Sammlung, Auswertung und dem Verkauf

Der 1959 geborene DP-Autor Dr. phil. Peter Löbbecke ist Professor für Kommunikationswissenschaften an der Fachhochschule Polizei Sachsen-Anhalt. Seit 1995 bildet er Polizeibeamtinnen und -beamte aus. Löbbecke studierte Soziologie und Erwachsenenpädagogik. Seine Arbeitsgebiete umfassen unter anderem die sichere Kommunikation im Internet, soziale Medien, die berufliche Sozialisation und den Schutz kritischer Infrastrukturen. Foto: Simone Löbbecke

Aus Platzgründen finden sich alle Quellen unter:
www.researchgate.net/publication/332950252_Sichere_Messenger_fur_die_Polizei

von Nutzerdaten leben. Smartphones sind extra betroffen: 2018 wurde festgestellt, dass 42,55 Prozent aller kostenlosen Apps aus dem Playstore Nutzerdaten an FB übermittelten.

Es ist auch nicht erforderlich, dass Nutzer über ein FB- oder Google-Konto verfügen. Die großen Firmen stellen Werkzeuge zur Verfügung, mit denen Programmierer Standardfunktionen in ihre Programme einbinden können – und damit „nebenbei" auch Tracker und ähnliches.

Alle gesammelten Informationen werden zu Nutzerprofilen verknüpft und diese wiederum mit Profilen anderer Menschen verbunden. Die Verknüpfung der Daten einer Person geschieht zum Beispiel über die Werbe-ID, über die jedes Smartphone verfügt, über Telefonnummern und andere persönliche Daten, oder auch über den Abgleich übermittelter Daten zu Nutzerinteressen. Die Verknüpfung mit anderen Personen geschieht unter anderem über Verbindungs- und Standortdaten, sogenannte Metadaten.

Metadaten im Blick

Telefonnummern, Werbe-ID oder Chat-Inhalte sind „einfache" Daten, die auf dem Gerät vorliegen beziehungsweise die der Nutzer übermitteln will. Viel wichtiger für die Erstellung von Persönlichkeitsprofilen sind aber Informationen, die unabhängig von den gesendeten Nachrichten anfallen, eben die bereits angesprochenen Metadaten: Wer chattet von wo mit wem wie lange – und sehr viel mehr. Metadaten sind so viel aussagekräftiger als die tatsächlichen Inhalte von Botschaften.

Aus fast allen Aktivitäten im Internet entsteht ein sehr fein strukturiertes Persönlichkeitsprofil für jeden Menschen mit zehntausenden von Einzeldaten, das tiefe Aufschlüsse über die Person erlaubt. Politische Überzeugung, Finanz- und Beziehungsstatus, Hobbys und vieles mehr lassen sich recht leicht errechnen. Berühmt wurde der Fall einer 15-Jährigen, deren Schwangerschaft der Werbewirtschaft eher bekannt war als ihren Eltern; der Datenmissbrauch der Firma Cambridge Analytica ist ein anderes Beispiel. Wer hat nicht schon im Internet unerwartete Werbung zu einem Produkt gesehen, das man kurz zuvor gegoogelt hatte. Entsprechend gefilterte Informationen – nach Schwangeren, politisch rechts oder links Stehenden, Homosexuellen, Rauchern ... – kann im Prinzip jeder kaufen, der das möchte. Und wenige Informationen reichen aus, um eine Person eindeutig zu identifizieren.

Kurzsichtige Nutzer

Der oft gehörte Satz „Ich habe nichts zu verbergen" ist kurzsichtig. Jeder

Mensch hat etwas zu verbergen, auch wenn er kein Krimineller ist: Den Kontostand, den Seitensprung, die Wahlentscheidung, die Bewerbung zur Konkurrenz, überhaupt alles Persönliche. Diese Privat- beziehungsweise Intimsphäre geht im Internet – ohne entsprechenden Schutz – schnell verloren: Werbung ist vielleicht „nur" lästig. Aber möchte ich, dass meine Schwangerschaft im Webseiten-Banner auftaucht, dass feststellbar ist, wann ich im Rotlichtviertel war oder dass ich regelmäßig Haschisch rauche? Sehr viel mehr geschieht bereits.

Kaum jemanden scheinen diese Tatsachen zu interessieren. Besonders problematisch ist die Situation aber für Polizisten, stehen sie doch für die Sicherheit (auch von Daten und Privatsphäre) ein und gehen mit schutzwürdigen Informationen um. Ein größeres Bewusstsein für sichere Kommunikation wäre zu wünschen.

Dienst ist Dienst

Für den dienstlichen Austausch stellt sich die Frage scheinbar nicht – dafür gibt es Funk und Telefon. Ich konnte jedoch zeigen, dass Polizisten sich mittels privater Smartphones über soziale Netzwerke, den FB-Messenger oder WA-Gruppen auch dienstlich austauschen. Es beginnt in der Ausbildung: „Morgen fällt die erste Stunde aus", und alle wissen Bescheid. Schon problematischer: Man schickt dem Prüfer per FB-Messenger eine Frage zur Polizeidienstvorschrift 100 (PDV 100) – einem VS-NfD-Dokument (Verschlusssache/Nur für den Dienstgebrauch) –, und sie wird im Klartext auf dem amerikanischen Firmenserver gespeichert und ausgewertet. Später geht es weiter: Die Kollegen erfragen Informationen, die auch auf dem Server landen: Man verabredet sich zu Fahrgemeinschaften. Das eigene Profil wird mit anderen verknüpft. Prinzipiell sollten in der Polizei solche Risiken, auch wenn sie auf den ersten Blick belanglos erscheinen, vermieden werden. Strenger formuliert: Grundsätzlich gehören dienstliche Inhalte und personenbezogene Informationen nicht in Kanäle, die nicht zu kontrollieren sind und die Daten und Metadaten zu Geld machen.

Im Alltag kann kaum streng zwischen privater und dienstlicher Kommunikation unterschieden werden, ein Verbot von Chats ist unrealistisch. Auch auf Systeme zu verweisen, die im Vergleich zu denen der großen Internetfirmen wenigstens ein etwas höheres Maß an Vertraulichkeit bieten wie etwa „Signal", „Threema", „Wire" oder „Telegram" hilft wenig: Auch sie haben bedenkenswerte Nachteile. Die Sicherheit von Telegram ist unklar. Die Verschlüsselung von Threema kann nicht unabhängig geprüft werden. Signal und Wire geben zwar Einblick in ihren Quellcode, benutzen aber zentrale, geschlossene Server. Man muss blind vertrauen, dass sie keine Metadaten sammeln und auswerten und macht sich technisch abhängig.

Verbieten?

Also doch ein Verbot? Es gäbe eine Alternative, und zwar die Nutzung von standardisierten Internet-Protokollen (Übertragungs-Standards) mit „freier" Software. „Frei" bedeutet, dass der Quellcode der verwendeten Software, der eigentliche Programmtext, für jeden zugänglich und nutzbar ist. Außerdem ist sie oft kostenlos oder preisgünstig.

Es gibt bewährte Standards, die auch für E-Mails verwendet werden. Diese erlauben allerdings nicht alle Funktionen moderner Messenger. Deshalb gibt es dafür eigene genormte Protokolle. Die beiden wichtigsten sind das schon lange existierende „Extensible Messaging and Presence Protocol" (XMPP) sowie das neu entwickelte „Matrix"-Protokoll. Beide sind vergleichbar, allerdings ist die Verschlüsselung bei Matrix noch nicht ganz ausgereift, was eher für die Nutzung von XMPP spricht, das deshalb hier im Vordergrund stehen soll. Selbst militärische Lösungen basieren auf XMPP. Die NATO prüft entsprechende Möglichkeiten. Auch WA beruht auf einem zum Zweck der Kommerzialisierung abgeschotteten XMPP. Beide Protokolle sind unabhängig von kommerziellen Anbietern. Prinzipiell kann jeder, also auch die Polizei, selbst als Internet-Dienst auftreten und einen sogenannten Server betreiben. Der Aufwand ist gering. Die Nutzer solcher Server können problemlos Nachrichten und Dateien mit den Nutzern aller anderen Anbieter oder Server austauschen. Bekannt ist das Prinzip von Telefon und E-Mail: Jeder kann jeden anrufen und jedem E-Mails schreiben – unabhängig von der Telefongesellschaft. Innerhalb von WA und ähnlichem bleibt man im geschlossenen System, dem man „blind" vertrauen muss.

Kontrollierte Kommunikationswege

Klar ist: Um eine vertrauenswürdige, auch für dienstliche Inhalte geeignete Kommunikation mittels moderner Messenger zu ermöglichen und den Abfluss der Metadaten verhindern zu können, muss man die Kommunikationswege kontrollieren können. Auch muss überprüfbar sein, ob die verwendete Software wirklich das tut, was sie verspricht. Bei „unfreien" („proprietären") Diensten ist das kaum gegeben: Entweder ist die ganze Software unprüfbar, oder die zentrale Schnittstelle (der Server).

Freie Software hat diese Probleme nicht. Ihr Quellcode kann jederzeit von Fachleuten dahingehend geprüft werden, was die Software tut, wie sie mit Daten und Metadaten umgeht, was gespeichert wird. Bei hohen Sicherheitsansprüchen kann die Organisation selbst den Quellcode in lauffähige Programme umsetzen und können unerwünschte Funktionen sicher ausgeschlossen werden. Leider tut sich der öffentliche Dienst schwer mit der Nutzung freier Software. Meist werden – zu Unrecht – Sicherheitsbedenken geltend gemacht.

Erkannte Sicherheitslücken schließen

Grundsätzlich ist nur Software „sicher", die regelmäßig weiterentwickelt wird und bei der erkannte Sicherheitslücken geschlossen werden – jeder kennt die häufigen Sicherheitsupdates des Betriebssystems. Das gilt ebenso für freie Software, und in der Tat wird auch diese weiterentwickelt, häufig intensiver als proprietäre. Oft besteht das Geschäftsmodell eines freien Softwareanbieters darin, die Software frei zur Verfügung zu stellen, um für Firmen und Organisationen kostenpflichtige Betreuung anzubieten.

Falsch ist das Vorurteil, freie Software sei leichter zu „hacken" als kommerzielle: In der Regel ist es nicht „die Software", die „gehackt" wird, sondern das System, in dem sie läuft. Es ist empfänglich für Angriffe aus dem Internet, wenn Sicherungsmaßnahmen versäumt werden – egal, ob freie oder proprietäre Software eingesetzt wird.

Lizenzprobleme und zusätzliche Kosten, etwa wenn sich die Arbeitsumgebung ändert (mehr Anwender), fal-

len meist weg. Software kann flexibel an eigene Bedürfnisse (Corporate Design, Spezialfunktionen, ...) angepasst werden. Das kann durch eigene sachverständige Mitarbeiter oder durch Auftragsvergabe geschehen – die Software bleibt für die Organisation kontrollierbar.

Komfortabel?

Wichtig ist die Frage: Gibt es Apps, die ähnlich komfortabel sind wie das beliebte WA, und die darüber hinaus die gebotene Sicherheit liefern? Die Antwort lautet: „Ja", wobei die komfortabelsten Chat-Apps zurzeit für Android-Smartphones existieren. Auch für andere Systeme gibt es aber zufriedenstellende Angebote.

Ich stelle nur kurz die Android-Apps vor, die ich selbst verwende, und verweise auf die umfangreiche Übersicht auf „Freie-Messenger.de". Es sind dies die (kostenlose) App „Pix-Art" und die App „Conversations" aus dem Play Store. Beide basieren ursprünglich auf demselben Quellcode und werden intensiv weiterentwickelt.

Sicherheitsniveau steigern

Polizisten nutzen regelmäßig WA oder den FB-Messenger privat und für dienstnahe Kommunikation, bauen aus Kollegen bestehende Gruppen auf und tauschen sich darin aus. Diese Grundfunktionen bieten selbstverständlich auch die freien Messenger. Beide verwenden für nicht-öffentliche Kommunikation standardmäßig eine unabhängig auditierte Ende-zu-Ende-Verschlüsselung („OMEMO"), die besonders hohe Sicherheit garantiert. Man kann prüfen, ob man auch wirklich mit dem gewünschten Gerät verbunden ist. Wie bei E-Mails kann man verschiedene Konten einrichten (privat/dienstlich). Von anderen Apps bekannte Funktionen wie Sprachaufzeichnung, Übermittlung von Bildern, Videos, dem eigenen Standort und so weiter sind ebenfalls vorhanden, so dass die Funktionalität anderen Messengern nicht nachsteht. Nur die Verbreitung ist noch geringer als zum Beispiel bei WA.

Um nun das Sicherheitsniveau zu steigern, könnte die Polizei eigene XMPP-Server aufbauen, deren Sicherheit der allgemeinen Polizei-Infrastruktur entsprechen würde. Sie könnte ihren Bediensteten Konten und Messenger zur privaten und – nach rechtlicher Prüfung – auch dienstlichen Nutzung anbieten (da sehr starke Verschlüsselung verwendet wird).

Wie bei E-Mails – aber viel sicherer – wären die Nutzer in der Lage, in- und außerhalb der Organisation zu kommunizieren. Die Nutzerbezeichnungen könnten frei und sogar unabhängig von Konventionen gewählt werden, so dass eine eindeutige Identifikation eines Nutzers außerhalb der Polizei zumindest erschwert würde (wobei sicher schnell bekannt wäre, dass der Server der Polizei gehört). Die Kosten und der Aufwand für ein solches System würden sich in engen Grenzen halten, wie die große Zahl privater, in der Freizeit betreuter Server belegt. Auch wenn die Nutzung solcher Angebote kaum kontrolliert werden kann, so ist doch zu erwarten, dass weniger Inhalte unsicher verschickt würden.

Umdenken wäre erforderlich

Allerdings wäre ein Umdenken seitens der Organisation erforderlich. Mit dem Abschied von proprietärer Software verlagert sich die Verantwortung für das Funktionieren und Nicht-Funktionieren auf sie selbst. Sie würde sich entscheiden müssen, ihre Software selbst zu prüfen und zu pflegen. Sie würde dafür eine Kontrolle über die eigene Kommunikations-Infrastruktur erlangen, wie es mit kommerzieller Software niemals möglich wäre. Wahrscheinlich würde auch die Nutzung der prinzipiell unsicheren E-Mail zurückgehen. Der Sicherheitsgewinn und praktische Nutzen dürfte mögliche Kosten bei weitem aufwiegen.

Interessierten empfehle ich die Website:
freie-messenger.de