Interview

Kein Zugriff für Unbefugte

[14.03.2018] In der täglichen Arbeit wird die E-Mail über kurz oder lang verschwinden. Sie wird von Messengern verdrängt. Ein Gespräch mit Marco Hauprich, Deutsche Post, über sichere, datenschutzkonforme Kommunikation über Kurznachrichtendienste.

Herr Hauprich, fast jeder Smartphone-Nutzer kommuniziert heute über Kurznachrichtendienste, in Deutschland meist über WhatsApp. Was spricht grundsätzlich dafür, Messenger auch in Behörden zu nutzen?

Dafür spricht vor allem die größere Effizienz durch schnellere und direktere Kommunikationswege. Ein Sachbearbeiter im Innendienst bekommt am Tag durchschnittlich rund 30 E-Mails. Deren Bearbeitung kostet ihn mindestens 45 Minuten Arbeitszeit. Die Verwendung eines Messengers macht die elektronische Kommunikation deutlich effektiver. Nach Untersuchungen namhafter Beratungsfirmen lässt sich so die Anzahl der Mails um die Hälfte reduzieren, was 15 Stunden Zeitersparnis im Monat bedeutet – also 35 Prozent mehr Produktivität. Nicht zu vergessen ist die deutlich größere Flexibilität gerade in der Kommunikation beispielsweise mit Außendienstmitarbeitern. Klar, es gibt Funk und Mobiltelefon, aber mit einem Messenger können Sie im Zweifel auch Pläne, Bilder oder Dokumente übermitteln. Da weiß der Mitarbeiter vom Grünflächenamt genau, welcher Baum zu fällen ist. Oder der Trupp vom Tiefbauamt kann anhand der Bilder eines frischen Straßenschadens schon abschätzen, ob er die Materialien bereits auf dem Wagen hat oder doch nochmal zum Bauhof fahren muss, um nur zwei Beispiele zu nennen.

Ist dies das Ende der E-Mail?

Das Ende glaube ich nicht. Aber es wird zu einer deutlichen Reduktion führen – und mal ehrlich, stöhnen wir nicht alle gelegentlich ob der E-Mail-Flut, ganz egal, ob dienstlich oder privat? Natürlich wird es immer noch Dinge geben, die per E-Mail ausgetauscht werden, aber das sind dann eher komplexe Vorgänge mit langfristigen Vorläufen. In der Organisation der täglichen Arbeit wird die E-Mail über kurz oder lang verschwinden. Schon jetzt bezeichnen 40 Prozent aller Führungskräfte in der Privatwirtschaft den Messenger als ihr wichtigstes Medium.

Warum sollten Kommunalverwaltungen dennoch auf WhatsApp in der Kommunikation verzichten?

Die öffentliche Hand hat eine ganz besondere Sorgfaltspflicht beim Umgang mit den ihr anvertrauten Daten. Das gilt umso mehr für persönliche Daten, die naturgemäß in den allermeisten Vorgängen einer Behörde irgendwo auftauchen, zum Beispiel im Jugendbereich oder bei der Grundsicherung. In dem Moment aber, wo diese Daten mit WhatsApp übermittelt werden, endet de facto die exklusive Herrschaft der Verwaltung über die Informationen. Denn die Server stehen irgendwo, in der Regel in den Vereinigten Staaten. Niemand kann ausschließen, dass amerikanische Nachrichtendienste dort Zugriff erhalten. Damit nicht genug, behält sich WhatsApp, beziehungsweise der Mutterkonzern Facebook, ausdrücklich die Auswertung der ebenfalls übermittelten Metadaten vor – also wer wann mit wem von wo aus kommuniziert hat. Eine Behörde, die WhatsApp für ihre Kommunikation nutzt, verletzt so gut wie alle Kernvorschriften des Bundesdatenschutzgesetzes (BDSG) und der EU-Datenschutz-Grundverordnung (EU-DSGVO).

„Wir speichern nichts, was wir nicht unbedingt zum Betrieb unserer App benötigen.“
Die Deutsche Post bietet mit SIMSme Business eine sichere Alternative. Was zeichnet den Dienst aus?

SIMSme Business hält sich stringent an die eben genannten Rechtsvorschriften. Alle unsere Server stehen sämtlich im Inland, es ist also nicht zu befürchten, dass plötzlich die NSA vor der Tür steht und die Festplatten mitnehmen will. Eine absolut sichere Ende-zu-Ende-Verschlüsselung der Nachrichteninhalte versteht sich von selbst. Aber auch darüber hinaus sind alle Nutzerdaten bei uns gut aufgehoben. Allein schon deshalb, weil wir nichts speichern, was wir nicht unbedingt zum Betrieb unserer App benötigen – ein echter Zero-Knowledge-Ansatz. Das gilt für sämtliche Metadaten, aber auch darüber hinaus. Der Telefonbuchabgleich zum Beispiel läuft bei SIMSme Business komplett verschlüsselt ab. Die Nummern werden auf dem Gerät des Nutzers im Hashwertverfahren codiert, in dieser Form auf unseren Servern mit dem Datenbestand verglichen und anschließend gelöscht. Der Nutzer kann außerdem besonders sensible Inhalte mit einer Selbstzerstörungsfunktion versehen. Jede Verwaltung kann davon ausgehen, dass kein Unbefugter Zugriff auf irgendwelche mit SIMSme Business ausgetauschten Informationen erhält.

Wie unterscheidet sich SIMSme Business von anderen verschlüsselten Messengern?

Wie schon erwähnt, handeln wir als deutsches Unternehmen auch nach deutschen und EU-Vorschriften. Des Weiteren ist zu bemerken, dass wir uns stringent an die Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) halten. Die Bedienung ist besonders komfortabel. So bieten wir mit dem Management Cockpit eine ausgesprochen einfach zu handhabende Administration der Anwendung auf Behördenebene. Über dieses Web-Interface lassen sich unter anderem Benutzerkonten einrichten oder löschen, Gruppen anlegen und verwalten oder Push-Kanäle für aktuelle Nachrichten bedienen. Zugleich ist das ein echtes Sicherheitsfeature gegen Missbrauch beispielsweise durch ausgeschiedene Mitarbeiter. Mit dem SIMSme Business Web Messenger bieten wir künftig auch die Möglichkeit, ganz bequem vom stationären Arbeitsplatz aus Nachrichten und Dateien zu versenden. Das erleichtert die Kommunikation zwischen Innen- und Außendienst ganz erheblich.

Mit welchen Kosten müssen Kommunen rechnen, die sich für SIMSme Business entscheiden?

Also zunächst einmal: SIMSme Business ist nicht kostenlos. Aber wir bieten für dieses Geld auch einiges, vor allem die bei Kommunen ungemein wichtige Datensicherheit. Wie hoch diese Kosten im Einzelfall sind, hängt von verschiedenen Faktoren ab. Wir verdienen unser Geld jedenfalls nicht mit den Daten der Nutzer, sondern mit Lizenzgebühren.

()

Dieser Beitrag ist in der März-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit,