Interview

Messenger in der Kritik

[17.12.2020] Im Zuge der Corona-Krise wurden im öffentlichen Sektor und an Schulen verstärkt Messenger-Dienste verwendet. Warum das Probleme mit sich bringt, berichtet Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen, im Kommune21-Interview.

Frau Thiel, während der Corona-Pandemie wurden vermehrt Messenger-Dienste wie WhatsApp als Kommunikationskanal zwischen Lehrern und Schülern genutzt. Wie bewerten Sie das?

WhatsApp ist aufgrund verschiedener datenschutzrechtlicher Mängel für die Kommunikation zwischen Lehrkräften und Schülern sowie im dienstlichen Austausch der Lehrkräfte untereinander ungeeignet. Bereits im Oktober 2018 habe ich daher in einem Schreiben alle Schulen in Niedersachsen sowie das Niedersächsische Kultusministerium darüber informiert, dass der Einsatz von WhatsApp im schulischen Kontext unzulässig ist. In der Anfangsphase der Corona-Pandemie im Frühjahr 2020 habe ich mich zwar dazu entschieden, den Einsatz von nicht vollständig datenschutzkonformen Messenger-Diensten und Videokonferenzsystemen an niedersächsischen Schulen im Einzelfall zu tolerieren und meine Bedenken zeitweise zurückzustellen. Dies war aber nur dem Umstand geschuldet, dass andernfalls die Kommunikation zwischen Lehrkräften und Schülern erschwert worden wäre und Online-Unterricht kaum hätte stattfinden können. Denn das Kultusministerium hat es in den vergangenen Jahren versäumt, ein verlässliches und datenschutzkonformes Angebot für den Fernunterricht bereitzustellen. Ich habe von Anfang an deutlich gemacht, dass dieser Zustand nicht von Dauer sein kann und das Kultusministerium im weiteren Verlauf aufgefordert, Alternativen zu WhatsApp ernsthaft zu prüfen. Jetzt befinden wir uns im Herbst. Das Ministerium ist zwischenzeitlich damit beschäftigt, datenschutzkonforme Alternativen zu finden.

Können Mitarbeiter in Kommunalverwaltungen Messenger-Dienste als Kommunikationstool nutzen oder wirft das ähnliche Probleme auf wie an den Schulen?

Auch hier gilt, dass Messenger-Dienste nur dann eingesetzt werden dürfen, wenn sie die Anforderungen der DSGVO und der deutschen Datenschutzgesetze erfüllen. Tatsache ist jedoch, dass etliche der verfügbaren Produkte diesen Vorgaben nicht gerecht werden. Auf einen Einsatz muss daher im öffentlichen Bereich verzichtet werden. Auch, weil öffentliche Stellen eine Vorbildfunktion einnehmen sollten.

„Schon bei der Installation des Programms wird häufig das Adressbuch des Nutzers hochgeladen."

Wo liegen die Schwachstellen, wenn es um den Einsatz im öffentlichen Sektor geht?

Wenn es datenschutzrechtliche Probleme bei der Nutzung eines Messenger-Dienstes gibt, dann bestehen diese unabhängig davon, ob ein Messenger bei einer Kommune, einer Behörde oder in einem Unternehmen zum Einsatz kommt. Eine erhebliche Hürde für den Einsatz einiger Messenger-Dienste stellt die Tatsache dar, dass schon bei der Installation des Programms häufig das Adressbuch des Nutzers hochgeladen wird, wodurch alle Kontakte für den Dienstbetreiber einsehbar und nutzbar werden. Problematisch ist dies vor allem in Bezug auf die Kontakte, die bisher den Messenger-Dienst nicht genutzt haben. Das wäre nur dann datenschutzkonform, wenn der Nutzer des Messengers zuvor das

Einverständnis aller Kontakte eingeholt hätte, was in der Praxis nahezu unmöglich sein dürfte. Die Übermittlung der Daten aus dem Adressbuch ist damit unzulässig. Um dieses Problem zu umgehen ist es denkbar, dass ein Smartphone mit einem leeren Adressbuch verwendet wird. Auch ist es möglich, durch Einstellungen im Messenger den Zugriff auf die Kontakte auszuschließen. Das hat zur Folge, dass Chats und die dazugehörigen Kontakte im Messenger nicht mehr mit dem im Adressbuch geführten Namen angezeigt werden, sondern nur noch mit der Mobilfunknummer. Bei WhatsApp findet sich sehr versteckt und nur für Nutzer, die den Adressbuch-Upload bereits deaktiviert haben (und den Zugriff auf die Kontakte dauerhaft deaktiviert lassen), die Möglichkeit, händisch im Messenger-Dienst eine Mobilfunknummer einzugeben und anschließend einen neuen Chat zu starten. Es gibt somit eine datenschutzkonforme Lösung für dieses Problem. Bei Threema ist die Synchronisation der Adressdaten hingegen standardmäßig deaktiviert. Problematisch ist zudem die Tatsache, das zahlreiche Anbieter von Messenger-Diensten personenbezogene Daten in Staaten außerhalb der EU übermitteln, ohne dass dafür eine Rechtsgrundlage vorliegt. Bei Threema befinden sich die Server zwar im Großraum Zürich, allerdings hat die EU-Kommission festgelegt, dass die Schweiz ein angemessenes Schutzniveau für personenbezogene Daten bietet. Ein besonderes Augenmerk sollte auch immer auf die Datenschutzhinweise der Messenger-Dienste gelegt werden. So ergibt sich beispielsweise aus der Datenschutzrichtlinie von WhatsApp, dass zahlreiche personenbezogene Daten der Nutzer zu kaum eingegrenzten Zwecken verwendet und auch an den Facebook-Konzern weitergegeben werden. Demnach werden Nutzerdaten in einer Art und Weise verarbeitet, die mit dem geltenden Recht wohl kaum in Einklang zu bringen ist.

Wie könnte eine Alternative zu diesen Messenger-Diensten aussehen, die bedenkenlos in Kommunalverwaltungen verwendet werden kann?

Ein entscheidender Faktor wäre es, wenn Dienste ausgewählt würden, die auf einen Abgleich der Kontaktdaten aus den Adressbüchern der Nutzer verzichten. Einige Messenger-Dienste bieten alternative Möglichkeiten der Kontaktaufnahme mit anderen Nutzern, zum Beispiel über einen QR-Code. Sofern andere Messenger-Dienste das gleiche Verfahren wie WhatsApp vornehmen, löschen zumindest einige nach eigenen Angaben die nicht registrierten Kontakte unmittelbar nach dem so genannten Negativabgleich.

Welche Kriterien muss eine Messenger-Lösung für Kommunen erfüllen, beispielsweise hinsichtlich des Datenschutzes?

Es muss gewährleistet sein, dass es Dritten nicht möglich ist, Gesprächs- und Chat-Inhalte mitzuverfolgen oder nachzulesen. Eine entsprechende Verschlüsselung muss sichergestellt sein. Häufig garantieren Messenger-Dienste die Verschlüsselung der Inhaltsdaten. Die so genannten Kommunikations-Metadaten – wer mit wem wie lange und wie oft kommuniziert – sind zunächst für die technische Umsetzung der Kommunikation erforderlich. Sie werden aber darüber hinaus häufig für andere Zwecke genutzt oder an andere Dienste weitergegeben. Dies müsste bei einem Messenger für den kommunalen Einsatz ausgeschlossen werden. Angesichts der jüngsten Entscheidung des Europäischen Gerichtshofs zur Ungültigkeit des Privacy-Shield-Abkommens zwischen der EU und den USA dürften inzwischen sämtliche Dienste ausscheiden, die Daten in die USA transferieren. Ob beim Einsatz von Messenger-Diensten auf der Grundlage von Standardvertragsklauseln und zusätzlichen Schutzmaßnahmen die Einhaltung des Datenschutzniveaus gewährleistet werden kann, erscheint sehr fraglich. Öffentliche Stellen sollten sich zwingend nach einem Anbieter umsehen, der Daten tatsächlich nur innerhalb der Europäischen Union verarbeitet, also im Geltungsbereich der DSGVO.
Ich kann nur immer wieder betonen, dass der Einsatz eines Messenger-Dienstes vorab eingehend geprüft

werden muss. Und zwar durch die Stelle, die einen solchen Einsatz plant. Außerdem wäre es natürlich denkbar, dass eine Kommunalverwaltung einen eigenen Messenger-Dienst betreibt.

()

Dieser Beitrag ist in der Ausgabe Dezember 2020 von Kommune21 im Schwerpunkt Social Media erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Social Media, Niedersachsen, Barbara Thiel, It-Sicherheit, Datenschutz, LfD