Polizei Niedersachsen

Messenger für interne Kommunikation

[28.05.2019] Für die interne Kommunikation nutzt die Polizei Niedersachsen einen eigens für sie angepassten Messenger-Dienst: NIMes. Die Behörde setzt dafür auf Bring Your Own Device. Inwiefern die Lösung als Modell für andere große Behörden, Organisationen oder Firmen dienen kann, erläutert NIMes-Projektleiter Marco Trumtrar.

Die Nutzung von kommerziellen Messengern wie WhatsApp, Threema oder Signal ist im Privatbereich weit verbreitet. Die Vorteile dieser schnellen, unmittelbaren und unkomplizierten Kommunikationsform liegen auf der Hand. Im Zuge der Einführung der Datenschutz-Grundverordnung (DSGVO) im Frühjahr vergangenen Jahres wurde allerdings bundesweit darüber diskutiert, ob eine Anwendung wie WhatsApp überhaupt datenschutzkonform betrieben werden kann. So müsste ein Nutzer die Einwilligung jeder Person, die er in seinem Adressbuch gespeichert hat, einholen, da deren Daten an WhatsApp übermittelt werden. Dieses Vorgehen ist im Alltag kaum vorstellbar, und es ist auch kaum anzunehmen, dass dies gelebt wird. Dennoch ist WhatsApp auch ein Jahr nach Einführung der DSGVO im Einsatz – allen datenschutzrechtlichen Bedenken zum Trotz.
Die Polizei Niedersachsen hat einen eigenen Weg beschritten und den internen Niedersachsen-Messenger NIMes beschafft (wir berichteten), um dem mutmaßlichen Missbrauch von unerwünschten Produkten zu begegnen. Der NIMes-Server steht beim Dienstleister der Polizei, Teilnehmer können nur in der Benutzerverwaltung der Polizei angelegt werden. Eine Besonderheit von NIMes ist aber, dass die Nutzung auf privaten Endgeräten der Mitarbeiterinnen und Mitarbeiter gestattet wurde.

Warum Bring Your Own Device?

Die Messenger-Kommunikation lebt von der jederzeitigen Verfügbarkeit des Dienstes. Zeitliche und räumliche Grenzen verschwimmen dabei zusehends. Im Rahmen der vorgeschaltenen fachlichen Analyse wurde festgestellt, dass ein Messenger auch außerhalb des unmittelbaren Dienstgeschehens zum Beispiel für Dienstplanungen genutzt werden soll. Ein System, bei dem das Endgerät und damit der Messenger zum Feierabend im Dienstgebäude verbleibt und an die nachfolgende Schicht übergeben wird, schied somit aus.
Um die Vorteile der Messenger-Kommunikation vollumfänglich nutzen zu können und die mutmaßlich verwendeten, aber unerwünschten Produkte konsequent aus der Polizei zu verbannen, blieb als Lösung die personenbezogene Ausstattung jedes Mitarbeiters mit einem dienstlichen, gemanagten, sicheren Endgerät oder die Freigabe der Nutzung auf den privaten Endgeräten der Beschäftigten.
Eine Ausstattung aller rund 23.000 Mitarbeiter mit dienstlichen Smartphones ist für die Polizei Niedersachsen unter Abwägung konkurrierender Bedarfe und unter Betrachtung einer Kommunikationsgesamtstrategie derzeit nicht zielführend. Damit rückte die Lösung in den Fokus, den Messenger für die Nutzung auf den privaten Endgeräten freizugeben. Die offizielle Verwendung von privaten Endgeräten zu dienstlichen Zwecken (Bring Your Own Device – BYOD) ist ein breit diskutiertes Thema und wird in den meisten Länderpolizeien abgelehnt. In der Polizei Niedersachsen ist es jedoch gelungen, zwischen den verschiedenen Beteiligten (Datenschutz- und Informationssicherheitsbeauftragte, Technikdienstleister, Mitarbeitervertretung, Innenministerium und Anwendern) einen Rahmen zu entwickeln, in dem BYOD – ausschließlich bezogen auf die Anwendung NIMes – ermöglicht wurde.

Wie funktioniert BYOD?

NIMes kann auf bis zu drei Endgeräten parallel betrieben werden. Dies können dienstliche PCs sowie dienstliche oder private Smartphones oder Tablet-PCs mit den Betriebssystemen Android oder iOS sein. Da NIMes auch für private Endgeräte freigegeben ist, muss die erforderliche Sicherheit in die Anwendung integriert sein, da das Endgerät als potenziell unsicher einzustufen ist.
Der Hersteller heinekingmedia hat sein Produkt Stashcat, das als Basis für NIMes dient, im Rahmen der Ausschreibung um wichtige und für die Polizei Niedersachsen notwendige Sicherheitsfunktionen erweitert. Dies sind eine vollständige und durchgehende Ende-zu-Ende-Verschlüsselung inklusive verschlüsselter Speicherung der Daten auf den Endgeräten, eine vollständige Kapselung der App auf dem Endgerät zur effektive Trennung von dienstlichen und privaten Daten sowie eine Funktion für die jederzeitige Fernlöschung der Daten durch einen Administrator, zum Beispiel bei Verlust des Endgeräts.
Durch die Implementierung sehr kurzer Löschfristen, einer Zwei-Faktor-Authentifizierung, der Anonymisierung von Push-Benachrichtigungen sowie der Entsperrpflicht der App durch Eingabe einer PIN und weiteren Detailverbesserungen sind die Voraussetzungen für die dienstliche Anwendung auf dem privaten Gerät geschaffen worden.
Neben den sicherheits- und datenschutzrechtlichen Voraussetzungen waren aber auch entsprechende organisatorische Rahmenbedingungen zu schaffen. Zu regeln waren die Freiwilligkeit der Nutzung des privaten Endgeräts, da BYOD nicht angeordnet werden kann, Belange des Mitarbeiterschutzes, wie die Verhinderung der jederzeitigen Erreichbarkeit, Belange der Arbeitszeitgestaltung sowie Kosten- und Haftungsaspekte. Die Mitarbeiter erhalten keine finanzielle Vergütung; neu ist aber eine Haftungsübernahme bei Beschädigung des Endgeräts im Dienst. Zur Regelung dieser Belange ist eine Dienstvereinbarung mit ergänzenden Erläuterungen zur Einhaltung von Ruhe- und Erholungszeiten zwischen dem Polizeihauptpersonalrat und dem Landespolizeipräsidenten geschlossen worden, die 2018 für einen Personalräte-Preis nominiert wurde.

Wo sind die Grenzen von NIMes?

NIMes hat klar definierte inhaltliche Grenzen. Zum einen sind Inhalte, die nach der Verschlusssachenanweisung als VS–NfD (Verschlusssache–Nur für den Dienstgebrauch) oder höher eingestuft sind nicht für die Versendung in NIMes zugelassen. Ebenso dürfen keine Inhalte verschickt werden, deren Bekanntwerden Leib und Leben einer betroffenen Person gefährden würde – Schutzstufe E nach dem Konzept der niedersächsischen Landesbeauftragten für den Datenschutz. Damit kann der größte Teil der dienstlichen Kommunikation über NIMes abgewickelt werden.
Eine weitere Grenze wird durch den bewusst beschränkten Nutzerkreis gesetzt. Als Messenger-Lösung dient NIMes der Kommunikation innerhalb der Polizei. Für die Kommunikation nach außen, also in Richtung anderer Polizeien des Bundes und der Länder, anderer Behörden oder in Richtung der Bürger, ist NIMes nicht gedacht. Das System ist mandantenfähig und grundsätzlich auch mit anderen Installationen auf Basis des Produkts Stashcat, wie etwa dem hessischen Messenger HePolChat (wir berichteten) vernetzbar. Hierfür müssten aber zunächst die organisatorischen Rahmenbedingungen angepasst werden.

NIMes und BYOD – ein Modell auch für andere?

Realistisch betrachtet ist ungeregeltes BYOD in nahezu allen Behörden und Firmen vertreten, da Mitarbeiter – teilweise offiziell geduldet, in den meisten Fällen aber unbemerkt vom Arbeitgeber – ihre privaten Geräte und Applikationen für dienstliche Zwecke nutzen. Das ist problematisch, da so dienstliche Daten unbemerkt die Behörde oder die Firma verlassen. Ein Verbot der Nutzung dieser Dienste kann

jedoch nicht effektiv durchgesetzt werden.
Die erfolgversprechendste Möglichkeit, den Missbrauch zu verhindern, ist das Angebot von möglichst gleichwertigen Alternativen. Für die interne Kommunikation kann NIMes daher als Modell für andere große Behörden, Organisationen oder auch Firmen dienen. Wenn die Aufgabenstellungen komplexer werden und beispielsweise auch externe Kommunikation, etwa mit Bürgern oder Firmen, hinzukommt, stößt dieses Modell jedoch an seine Grenzen.
Das Zulassen des Einsatzes privater Endgeräte kann im Ergebnis eine Stärkung der Informationssicherheit und des Datenschutzes darstellen, wenn ein leistungsstarkes, sicheres System bereitgestellt wird, in dem klare, durchsetzbare Regeln definiert werden und damit eine ungeregelte und unkontrollierbare Nutzung verdrängt wird.

()

Stichwörter: Innere Sicherheit, BYOD, Messenger, NIMes, Polizei Niedersachsen