IT-Sicherheit

Mobile Integrität wahren

[28.01.2021] Wenn Mitarbeiter behördliche Informationen über private Messenger-Dienste austauschen, drohen Sicherheitslücken und DSGVO-Verstöße. Eine Lösung, die auf einer Container-Technologie basiert, kann mobile Kommunikation nach höchsten Standards schützen.

Termine vereinbaren, Personal koordinieren, Dokumente bearbeiten, sich mit anderen Dezernaten austauschen – eine schnelle Kommunikation und flexibles Arbeiten können den Behördenalltag sehr erleichtern. Besonders im Außendienst ist es von Vorteil, wenn Ordnungsämter, Forstverwaltung oder Aufsichtsbehörden von unterwegs aus tätig sein können: Der Mitarbeiter fotografiert die vorgefundene Situation, macht sich Notizen, greift auf Fachanwendungen im Behördennetzwerk zu, hat direkte Akteneinsicht und kann Dateien via E-Mail oder Messenger an seine Kollegen weiterleiten.
Andererseits lauern beim mobilen Arbeiten zahlreiche Risiken. Gerade wenn Mitarbeiter private Geräte im Rahmen von Bring Your Own Device (BYOD) für dienstliche Aufgaben verwenden oder dienstlich bereitgestellte Geräte nach dem COPE-Prinzip, kurz für Corporate Owned, Personally Enabled, auch privat nutzen dürfen. Veraltete Betriebssysteme, unsichere WLAN-Verbindungen und die Nutzung von Apps, die es mit der Privatsphäre nicht so genau nehmen, sind häufig Einfallstore für Cyber-Kriminelle und der Grund für Verstöße gegen die Datenschutz-Grundverordnung (DSGVO).

Systematische Verstöße gegen Datenschutz-Grundverordnung

Bei Verletzungen der Datenschutzbestimmungen drohen den Verantwortlichen in der öffentlichen Verwaltung nicht nur disziplinarische Maßnahmen, sondern aufgrund ihrer Vorbildfunktion auch ein Vertrauensverlust seitens der Bürger. Trotzdem mussten sogar Bundesbehörden zu Beginn der Corona-Pandemie ihre IT-Infrastruktur für private Geräte öffnen, denn sie konnten nicht allen Mitarbeitern dienstliche Mobilgeräte zur Verfügung stellen.
Problematisch sind weit verbreitete Dienste wie WhatsApp, die in Behörden viel genutzt werden. Die App liest die Adressbücher der Mitarbeiter mit den Kontaktdaten von Kollegen und Lieferanten aus und gibt die Daten an die Konzernmutter Facebook weiter. Darüber hinaus erfasst WhatsApp auch Metadaten, etwa GPS-Daten, Absturzberichte und Nutzerverhalten. Viele Behörden haben für diese Dienste keine Nutzungsregelungen aufgestellt oder dulden sie stillschweigend. Dabei hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) dem Messenger-Dienst zuletzt wiederholt systematische Verstöße gegen die Datenschutz-Grundverordnung vorgeworfen und gerade deutsche Bundesbehörden daran erinnert, dass ein offizieller Einsatz nicht möglich ist.

Private und dienstliche Daten trennen

Trotz der bekannten Sicherheitsmängel läuft die informelle dienstliche Kommunikation innerhalb von Behörden häufig über WhatsApp und andere Dienste ab. In der Praxis wird privat und dienstlich unter Kollegen nicht sauber getrennt – mit weitreichenden Konsequenzen. Besonders kritisch wird die Lage, wenn zum Beispiel auf Ministerialebene oder bei Polizeibehörden Informationen mit der Einstufung „Verschlusssache – nur für den Dienstgebrauch (VS-NfD)“ mobil verarbeitet werden sollen.
Der einzige Ausweg ist eine strikte Trennung zwischen privaten und dienstlichen Daten auf den Mobilgeräten der Mitarbeiter. Dabei ist es unerheblich, ob Behörden die Nutzung privater Smartphones

und Tablets für dienstliche Zwecke erlauben oder umgekehrt. Eine Kommunikationslösung, die auf einer Container-Technologie wie SecurePIM Government basiert, speichert Behördendaten in einem verschlüsselten Bereich, sodass diese strikt von persönlichen Daten und Kontakten getrennt sind. Auch jeglicher Datentransport ist dabei Ende-zu-Ende verschlüsselt. Für den Mitarbeiter, der gerade seine dienstlichen E-Mails abruft, ist es nicht möglich, aus der abgesicherten App heraus auf persönliche Anwendungen zuzugreifen. Umgekehrt können auch keine privaten Anwendungen auf die dienstlichen Inhalte zugreifen.

Nutzerfreundlich mobil arbeiten

Eine moderne Lösung für die mobile Kommunikation muss den Mitarbeitern ein Büro in Miniformat an die Hand geben, mit dem sie ihr Tagesgeschäft problemlos erledigen können. Damit stehen zum Beispiel alle aus Outlook und Notes bekannten Funktionen wie E-Mails, Kalender, Kontakte, Aufgaben und Notizen zur Verfügung. Auch ein gehärteter Browser für webbasierte Fachanwendungen und sicheres File-Sharing sind ein Muss. So können Behördenmitarbeiter Dokumente sicher abrufen, bearbeiten und wieder ablegen. Die mobile Kommunikationsanwendung SecurePIM Government des Unternehmens Virtual Solutions bietet zusätzlich einen Messenger inklusive verschlüsselter Telefonie, der neben Einzel- auch Gruppen-Chats, Videotelefonie, Sprachanrufe und Dokumentenversand beinhaltet.
Für Behörden, die mit Geheimhaltungsstufe VS-NfD arbeiten müssen, gibt es die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für das Betriebssystem iOS zugelassene und für das Betriebssystem Android freigegebene Systemlösung SecurePIM Government SDS. Über 25 Bundesbehörden haben diese in den vergangenen drei Jahren auf Tausenden von Endgeräten ausgerollt. Leistungsstarke Tablets, wie zum Beispiel ein iPad Pro, bieten den Mitarbeitern jetzt auch für Verschlusssachen einen vollwertigen, flexiblen Arbeitsplatz. Die Mitarbeiter können so bequem und nutzerfreundlich mobil arbeiten und kommunizieren – die Integrität und Sicherheit der Behördendaten ist jederzeit gewährleistet.

()

Dieser Beitrag ist in der Ausgabe Januar 2021 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Virtual Solution