Der Senator für Inneres

Bremen, 29.08.2018
Herr Schmauder
Tel. 361-96577

Vorlage für die Sitzung der
STAATLICHEN Deputation für Inneres
am 13.09.2018

Vorlage Nr. 19/208
Zu TOP 5 Teil A der Tagesordnung

Sachstandsbericht zum Beschluss 19/959 "Fahnden, orten, sichtbar machen! - Mehr Tempo und Sicherheit durch effektive Nutzung mobiler Endgeräte bei der Polizei

A. Problem

Die Bürgerschaft (Landtag) hat den Senat mit dem o.g. Beschluss aufgefordert, ein Konzept zur modellhaften Einführung von mobilen Endgeräten und zum Aufbau eines Messenger-Dienstes für den Polizeivollzugsdienst in Bremen und Bremerhaven zu erstellen und der staatlichen Deputation für Inneres binnen eines halben Jahres nach Beschlussfassung vorzustellen.

B. Sachstand

Während der o.a. Beschluss schwerpunktmäßig auf die Nutzung von Messenger-Diensten abhebt, wird das komplexe Thema „Mobiles Arbeiten“ bei der Polizei Bremen konzeptionell breiter aufgefasst. Zur Bearbeitung werden in der Polizei fünf Themenbereiche unterschieden:

a) Nutzung von mobilen Arbeitsplatz-PCs
b) Nutzung eines Personal-Informations-Managements (PIM)
c) Verwendung eines Messenger-Dienstes für die Spezialeinheiten
d) Verwendung eines Messenger-Dienstes für alle Organisationseinheiten
e) Nutzung von polizeilichen Informations- und Datensystemen vor Ort (Polizei-Apps)

Beim Themenbereich a) geht es um die Bereitstellung eines mobilen Arbeitsplatzes, der dieselben Möglichkeiten wie der stationäre Arbeitsplatz-PC im Büro der Mitarbeiterinnen und Mitarbeiter bietet.
Bei den Themen b) bis e) sind die mobilen Endgeräte (Smartphones/Tablets) und die damit verbundenen strategischen Grundentscheidungen (Geräteauswahl, IT-Sicherheit/BYOD sowie Personal und Kosten) das verbindende Element. Hier sind neue datenschutzrechtliche Anforderungen (sowie Geheimschutz) an die Gerätesicherheit zu stellen und müssen bereits bei der Grundentscheidung bereits mit einbezogen werden.

In allen Themenbereichen sind in den vergangenen Monaten signifikante Fortschritte erzielt worden, die nachfolgend dargestellt werden.

a) Nutzung von mobilen Arbeitsplatz-PCs

Im Kontext Telearbeit hat die Polizei Bremen eine technische Lösung beschafft, die den sicheren Zugang von außen in die hiesige IT-Infrastruktur ermöglicht. Diese Lösung wurde sowohl durch die IT-Sicherheit als auch durch das Haus LfDI bereits begutachtet. In Kombination mit verschiedenen technischen und organisatorischen Maßnahmen zur weiteren Verbesserung von Datenschutz und IT-Sicherheit ist diese Lösung zwischenzeitlich abgestimmt. Das System ist bereits im Betrieb.

Über diese Lösung wird auch der Zugriff mit Hilfe von mobilen Arbeitsplatz-PC (Laptops) möglich. Derzeit wird diesbezüglich ein Testbetrieb mit einer kleinen Anzahl von Geräten mit Schwerpunkt für mobile Befehlsstellen und Spezialeinheiten durchgeführt. Eine Datenschutz-Folgeabschätzung durch die Datenschutz-Nord GmbH ist beauftragt. Anhand derer soll noch in 2018 eine Verfahrensbeschreibung und notwendige Maßnahmen mit dem Hause LfDI abgestimmt und das Verfahren in den Echtbetrieb übergeben werden. Geplant ist, zunächst mit 25 mobilen Arbeitsplätzen zu beginnen und diesen Bestand sukzessive zu erhöhen. Neben den o.a. Anwendungsbereichen sind auch die Ausstattung der Polizeiboote, die Nutzung für Schwerlast- oder sonstige Kontrollstellen, die Abdeckung von Rufbereitschaften und diverse weitere Nutzungsmöglichkeiten denkbar.

b) Nutzung eines Personal-Information-Managements (PIM)

Mit dem Begriff Personal-Information-Management wird in der IT der mobile Zugriff auf Kontakte, Kalender und eMail bezeichnet. Derzeit verfügen in der Polizei Bremen rund 45 Führungskräfte über ein spezielles, dienstlich geliefertes Smartphone bzw. ein Tablet, mit dem diese Informationen mit den dienstlichen Systemen synchronisiert werden können. Mithin haben diese Mitarbeiterinnen und Mitarbeiter auch unterwegs die Möglichkeit neben ihren dienstlichen Kontakten das dienstliche Outlook für die Bearbeitung von eMails inkl. der Kalenderfunktion zu nutzen. Diese Geräte werden in einem Mobile-Device-Management-System durch die IT-Abteilung der Polizei verwaltet und administriert. Das Verfahren wurde Mitte 2017 etabliert und läuft störungsfrei.

c) Verwendung eines Messenger-Dienstes für die Spezialeinheiten

Bereits seit mehreren Jahren gibt es auf föderaler Ebene Bestrebungen, die Spezialeinheiten mit einem einheitlichen Messenger-System auszurüsten, das neben der reinen Messenger-Funktion auch Aspekte wie Ortung und Lagedarstellung einschließt. Das Vorhaben wird unter der Bezeichnung EKUS (Einsatz-, Kommunikations- und Unterstützungs-System) geführt. Die Leistungsbeschreibung wurde auf Bundesebene abgestimmt. Mit einer Einführung wird aber nicht in den kommenden 2-3 Jahren gerechnet. Im weiteren Entwicklungsprozess ist geplant, EKUS auch für die Bereitschaftspolizeien und nachfolgend auch für den übrigen Einsatzdienst verfügbar zu machen.

Um den hiesigen Spezialeinheiten für die Zwischenzeit bis zur Einführung von EKUS eine nutzbare Lösung zur Verfügung zu stellen, ist die Polizei Bremen der länderübergreifenden Entwicklungskooperation „SE-Netz“ beigetreten. SE-Netz ist einer der Kandidaten für die Software-Lösung, die einmal als EKUS bundesweit eingesetzt werden soll. 90 dienstliche Endgeräte mit gehärtetem Betriebssystem wurden um den Jahreswechsel 2017/2018 beschafft. Die Landespolizei Niedersachsen betreibt im Rahmen einer Kooperation das nötige Zentralsystem und administriert auch die bremischen Endgeräte. Das System ist einsatzbereit, soll aber auf Wunsch der Mitarbeitenden für Bremen noch in einzelnen Details angepasst werden, bevor der Wirkbetrieb demnächst beginnt.

d) Verwendung eines Messenger-Dienstes für alle Organisationseinheiten

Bereits seit 2017 setzt die Polizei Bremen das Messenger-System „StashCat“ in einem Pilotbetrieb ein. Eingebunden sind bisher die o.a. dienstlichen Handys/Tablets der Führungskräfte, das Lagezentrum, die Leitstelle OPB, die Pressestelle sowie der Zivile Einsatzdienstes und einzelne Funktionsträger.

Ab August 2017 begann eine Arbeitsgruppe ein Einführungskonzept unter Einbindung weiterer Nutzergruppen zu erarbeiten. Die Arbeitsgruppe hat zwischenzeitlich mehrere Erhebungen bzgl. der taktischen Bedarfe sowie zur benötigten Anzahl der Geräte durchgeführt. Im Kern werden folgende Funktionen benötigt:

- Austausch von Text-, Sprach- und Videonachrichten
- Einzel- und Gruppenchats
- Übermittlung von Bildern, Videos und Dateien diverser Formate
- Georeferenzierung / Standortübermittlung und –visualisierung
- Kompatibilität mit Lösungen benachbarter Organisationen (namentlich NDS, BuPol)
- Push-Notification (der Eingang neuer Nachrichten wird, z.B. durch ein Pop-Up, mitgeteilt)
- Eigenes Branding möglich (Die App kann mit dem „Corporate Design“ der Polizei Bremen individualisiert werden)
- Chat-Bot-Option (mit Chat-Bots können automatisierte Funktionen genutzt werden. Beispiel: bestimmte Eingaben, z.B. Name + Geburtsdatum, in einem bestimmten Chat rufen im Hintergrund z.B. eine INPOL-Abfrage hervor – das Ergebnis wird im Chat dargestellt)
- EU-DSGVO-Konformität
- Ende-zu-Ende-Verschlüsselung
- Hosting on- Premise (der Server kann lokal im Netz der Polizei betrieben werden)
- Kompatibilität mit Mobil-Device-Management (Fernadministration der Endgeräte)
- Sicherheitscontainer (Zugriffsschutz durch den App-Hersteller)
- Verschlüsselung der Inhalte auf Server und Endgerät
- Datenlöschung nach Zeitablauf (Fristen)
- Leistungsfähige Administrationstools

Im Ergebnis kommt die Arbeitsgruppe Messenger zu dem Ergebnis, dass StashCat für die bestehenden Bedarfe geeignet ist und daher weiter Verwendung finden könnte. Für einen Echtbetrieb wäre allerdings noch der Aufbau der lokalen Server-Lösung im Netz der Polizei Bremen erforderlich.

Im Verlauf der konzeptionellen Befassung mit dem Thema wurde bekannt, dass Dataport derzeit an der Entwicklung eines eigenen Messenger-Systems namens dMessenger arbeitet. Am 05.06.2018 wurde das System bei der Polizei Bremen vorgestellt. Die Basis bildet der Messenger „Teamwire“, der auch bei der Polizei in Bayern eingesetzt wird. Teamwire hat gegenüber Dataport die API (Application programming interface = Programmierschnittstelle) offengelegt und ermöglicht damit die Erweiterung von Teamwire mit zusätzlichen Optionen. So plant Dataport die Integration von automatisierten Fahndungsabfragen über die Chat-Bot-Funktion (s.o.). Damit würde sich der dMessenger bereits in Richtung eines Abfragetools/PolizeiApp entwickeln.

Zudem hat Dataport angekündigt, eine Kopplung der Smartphones mit dem TETRA-Digitalfunk zu erarbeiten. Dies ist insofern besonders interessant, da damit die 2-Faktor-Authentifizierung wirksam umgesetzt würde und ein abhanden gekommenes Smartphone mit dienstlichen Daten für den böswilligen Finder/Entwender unmittelbar wertlos würde.

Vor diesem Hintergrund ist die finale Entscheidung, welches Messenger-System für die Polizei Bremen zum Einsatz kommen soll, noch nicht gefallen. Bis Jahresende will Dataport eine wirkbetriebsfähige Version des dMessenger vorstellen. Nachfolgend wird dann geprüft, ob dMessenger eine sinnvolle Alternative zu StashCat darstellt.

e) Nutzung von polizeilichen Informations- und Datensystemen vor Ort (Polizei-Apps)

Neben dem Messenger sind für die polizeiliche Aufgabenwahrnehmung vor allem polizeispezifische Auskunfts- und Datenverarbeitungsanwendungen interessant. Die Entwicklung und insbesondere die Pflege (ständige Anpassung an Weiterentwicklungen des Betriebssystems des Endgerätes) ist ein komplexes und arbeitsintensives Unterfangen. Die Polizei Bremen verfügt über keine entsprechend qualifizierten Mitarbeiterinnen und Mitarbeiter, so dass hier lediglich eine Fremdvergabe in Betracht kommt. Da damit üblicherweise einmalige Kostenaufwände im mittleren sechsstelligen Bereich und jährliche Pflegekosten im hohen fünfstelligen oder unteren sechsstelligen Bereich verbunden sind, wurde diese Option nicht ernsthaft geprüft.

Der hiesige Fokus liegt aktuell auf zwei Optionen, die sich aus der länderübergreifenden Zusammenarbeit der Polizeien ergeben:

1. Die Polizei Bremen ist Teil der Kooperation zur Weiterentwicklung des Vorgangsbearbeitungssystems @rtus. Dataport entwickelt das VBS ständig weiter und hat Anfang 2018 auch mit der Entwicklung einer mobilen Version begonnen. Zusätzliche Kosten entstehen hier zunächst nicht, da die Entwicklung aus den Ressourcen der o.a. Kooperation finanziert wird. Zwischenzeitlich liegt eine modellhafte Vorführversion vor, die den Funktionsumfang plastisch darstellt, ohne tatsächlich die Funktionen zu beinhalten. Bis Jahresende 2018 will Dataport eine erste Alpha-Version bereitstellen können. Neben der Vor-

Ort-Erfassung von relevanten Daten für die Berichterstattung, Scan- und Fotofunktionen, sollen auch die Abfragemöglichkeiten der Desktop-Version von @rtus enthalten sein, so dass Fahndungsinformationen vor Ort unmittelbar verfügbar würden. Anforderungen an die Endgeräte hat Dataport bisher nicht formuliert, ggf. soll auch ein Gesamtpaket aus Endgerät und Software angeboten werden.

2. Die Bundespolizei hat den übrigen Polizeien des Bundes und der Länder angeboten, an den dort mit einem Dienstleister entwickelten Applikationen teilzuhaben. Derzeit sind zwei Apps mit Abfragemöglichkeiten in den Fahndungssystemen sowie zur Überprüfung von Dokumenten verfügbar. Die Nutzung dieser Option ist abhängig von der Entscheidung über die Endgeräte. Die Bundespolizei fordert von den Teilnehmern die Nutzung von Android-Geräte mit Samsung Knox und verbietet zudem Bring-your-own-Device (BYOD).

Im Anschluss an die Entscheidungen zu den nachfolgend dargestellten Fragen zu Endgeräten, IT-Sicherheit/BYOD sowie Personal und Kosten werden die notwendigen Maßnahmen zur Nutzung der o.a. Optionen eingeleitet.

Mobile Endgeräte

Bei den Fragen der Nutzung von Smartphones und Tablets müssen strategische Grundentscheidungen getroffen werden. Um zu vermeiden, dass mehrere Geräte vorgehalten werden müssen, ist ein Endgerät zu wählen, das zumindest für die eigene Lebensdauer von ca. 4 Jahren den Anforderungen in allen Punkten genügt und damit hinreichende Planungssicherheit bietet. Da die Innovationszyklen aktuell sehr kurz sind, sind die zu treffenden Entscheidungen strategisch besonders bedeutsam. Mit dem Serverbetrieb im eigenen Netz sowie die Ende-zu-Ende-Verschlüsselung sind wesentliche Risiken bereits wirksam ausgeschaltet. Als potenzielles Angriffsziel bleibt in Bezug auf die polizeilichen Daten im Kontext mobiles Arbeiten daher das Endgerät. Umso mehr ist hier besondere Sorgfalt notwendig.

1. IT-Sicherheitsbedarfe/gehärtete Betriebssysteme/BYOD

Ein Risiko setzt sich grundsätzlich aus Eintrittswahrscheinlichkeit und Folgen zusammen. Je schwerwiegender die Folgen, desto massiver muss die Möglichkeit des Eintritts reduziert werden, um ein tragfähiges Risiko zu erhalten. Der Abfluss oder die Manipulation von polizeilich erhobenen und verarbeiteten personenbezogenen Daten wird von der Polizei Bremen grundsätzlich als schwerwiegendes Schadensereignis im Sinne einer Risikobewertung wahrgenommen. Insofern sind im Kontext mobiles Arbeiten und vor dem Hintergrund der o.a. Vorrangigkeit der Endgeräte als potenzielles Angriffsziel besondere Maßnahmen der Sicherung zu ergreifen. Technische Maßnahmen sind organisatorischen Maßnahmen dabei grundsätzlich vorzuziehen. Notwendig erscheint aus hiesiger Sicht:

- Verwaltung der Endgeräte in einem zentralen Mobile-Device-Management

- Einsatz von Endgeräte mit gehärteten Betriebssystemen

Bring-your-own-device (BYOD)

Diese beiden Aspekte schließen zwangsläufig bereits die so genannten „Bring-your-own-device“-Lösungen aus. Das BSI hat für BYOD noch einen Grundschutzkatalog vorgestellt, stellt aber in seinem Überblickspapier klar, dass BYOD überhaupt nur denkbar ist, wenn

- aktuelle Virenschutz-Programme (soweit verfügbar) verwendet werden,
- alle Sicherheitspatches zeitnah eingespielt werden,
- jedes Endgerät ausschließlich durch den jeweiligen Mitarbeiter genutzt wird,
- der Zugriff auf die Endgeräte angemessen geschützt wird, z. B. durch starke Passwörter, und
- alle lokal gespeicherten Daten verschlüsselt werden.

Dieses Maßnahmenpaket könnte nur sichergestellt werden, wenn jedes Handy der Mitarbeiterinnen und Mitarbeiter in das Mobile Device Management der Polizei eingestellt und von dort administriert wird. Das ist weder im Sinne der Mitarbeitenden, noch personell leistbar (Hinweise zum personellen Aufwand für die Administration der Technik sind im Abschnitt 3 d dargestellt).

In seiner 28. Sitzung hat der Unterausschuss Polizeiliche Informations- und Kommunikationsstrategie und -technik des Arbeitskreises II „Innere Sicherheit“ der Ständigen Konferenz der Innenminister und –senatoren der Länder am 22./23.03.2016 in Hamburg den Polizeien des Bundes und der Länder zudem empfohlen, aufgrund der technischen Risiken und komplexen rechtlichen Voraussetzungen von der Nutzung privater mobiler Endgeräte (Bring Your Own Device / BYOD) für den Einsatz im polizeilichen Bereich grundsätzlich abzusehen.

Die aktuell durch den Senator für Inneres erarbeitete und in Abstimmung befindliche *Richtlinie zur Nutzung mobiler IT für die Polizeien des Landes Bremen* verdeutlicht: „Die Nutzung von privaten mobilen Endgeräten zu dienstlichen Zwecken – auch unter dem Schlagwort „Bring Your Own Device (BYOD)“ bekannt – ist untersagt!“

Die Polizei Niedersachsen will seinen Messenger auch im Rahmen einer BYOD-Lösung den Mitarbeitenden zur Nutzung anbieten. Der Landesbeauftragte für den Datenschutz Niedersachsen hat sich dazu eindeutig positioniert und lehnt dies im Schreiben vom 10.01.2018 ab: „Der zentrale Kritikpunkt bestand zu diesem Zeitpunkt in der geplanten Verwendung privater Endgerate für dienstliche Zwecke (u. a. Datenerhebung und -Verarbeitung zur Strafverfol-gung) und dem daraus resultierenden, nicht mit datenschutzrechtlichen Vorgaben in Einklang zu bringenden Ansatz "bring your own device" (BYOD).“

Eine BYOD-Lösung wird daher aktuell nicht verfolgt. Die Entwicklungen werden weiter interessiert betrachtet.

Gehärtete Betriebssysteme

Das Bundesamt für Sicherheit in der IT definiert den Begriff „Härten“: die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind. Mobile Betriebssysteme wie Android sind bewusst so gestaltet, dass sich den Entwicklern ein breites Spektrum an Möglichkeiten bietet, für ihre App auf Standardfunktionen des Systems zurückzugreifen. Zwangsläufig bieten sich dadurch auch für den Angreifer, der sich im Besitz des Gerätes befindet und z.B. durch Überwindung der PIN bereits Zugriff auf das System erlangt hat, viele Möglichkeiten des Angriffs auf Datencontainer, in denen die dienstlichen Daten aufbewahrt werden, selbst wenn diese brauchbar geschützt sind. So kann sich der Angreifer durch einen so genannten Root die höchst möglichen Zugriffsrechte auf das Betriebssystem Android verschaffen und ist anschließend im Grunde vergleichbar mit dem Administrator bei Windows-Systemen. Anschließend können Systemfunktionen, die eine App verwendet, manipuliert werden, was im Worst Case den Zugriff auf die dienstlichen Daten eröffnet. An dieser Stelle setzen gehärtete Betriebssysteme an, indem sie Angriffspunkte reduzieren, mögliche Werkzeuge entfernen, Rechte stark einschränken. Der wesentliche Nachteil an einem gehärteten Betriebssystem ist, dass mit jeder neuen Version des Ursprungsbetriebssystems auch eine neue Version der gehärteten Variante und Lösungen für neue Features erarbeitet werden müssen. Dadurch entstehen hohe Kosten für die Softwarepflege.

Die Polizei Niedersachsen hat sich für die Verwendung von BizzTrust auf ihren dienstlichen Mobilgeräten entschieden. BizzTrust, ein gehärtetes Betriebssystem, ist eine Entwicklung des Fraunhofer-Instituts für Sichere Informationstechnologie in Kooperation mit der Sirrix AG, einem Unternehmen für Enterpreise Security für Unternehmen und Behörden. SE-Netz, der eingesetzte Messenger für Spezialeinheiten und vermutlich Grundlage für das künftige Einsatz- Kommunikations- und Unterstützungssystem (EKUS), kommt auf BizzTrust-Handys zum Einsatz. Die unter c) bereits angeführten 90 beschafften Geräte sind daher natürlich ebenfalls mit BizzTrust ausgestattet.

Eine Alternative ist das von der Bundespolizei favorisierte „Samsung Knox“. Die Architektur von Knox ist BizzTrust ähnlich. Aktuell befindet sich die Polizei in Gesprächen mit der Fa. Samsung bzgl. dieser Lösung. Am 21.08.2018 ist die Technik durch Samsung vorgestellt worden. Nachfolgend sollen die Vor- und Nachteile der beiden Systeme vergleichend bewertet werden.

Im Hinblick auf die Endgeräte und deren konkrete Ausgestaltung (Hardware/Betriebssystem) ist daher bisher bei der Polizei Bremen noch keine Entscheidung gefallen.

Fazit

- Die Polizei Bremen hat in allen Themenbereichen signifikante Fortschritte erzielt.
- Der Messenger-Dienst für die Spezialeinheiten ist technisch einsatzbereit. Die Geräteanzahl soll noch erhöht werden.
- Auf den vorhandenen dienstlichen Smartphones ist ein bedarfsgerechter Messenger in Betrieb. Die Ausweitung der Messenger-Nutzung auf weite Teile der Mitarbeiterschaft ist noch nicht erfolgt. Vor weiteren Schritten ist der Aufbau einer lokalen Server-Infrastruktur notwendig. Ein Wechsel der Applikation ist denkbar, wenn Dataport seine gesteckten Ziele erreicht.
- Zur Entwicklung eigener Apps fehlt hier das fachliche Know-how. Die Polizei Bremen setzt daher auf die @rtus-Kooperation und prüft auch die mögliche Nutzung der Apps der BuPol.
- Die finale Auswahl der Endgeräte ist noch nicht erfolgt.
- Der Senator für Inneres hat sich für die Nutzung von gehärteten Betriebssystemen entschieden und verfolgt aktuell keine BYOD-Lösung. Die Entwicklungen werden weiter interessiert betrachtet.
- Für eine Umsetzung werden (je nach Szenario) fünf- bis sechsstellige Beträge sowie Personalressourcen im Umfang von 2,5 – 4 VZE benötigt.

C. Beschlussvorschlag

Die staatliche Deputation für Inneres nimmt den Sachstandsbericht zur Kenntnis.