03
Mai/Juni
2016

61. Jahrgang
A 5625 | € 7,00
ISSN 0722-5962

www.polizei-verkehr-technik.de

pvt

POLIZEI VERKEHR + TECHNIK

Fachzeitschrift für Polizei- und Verkehrsmanagement, Technik und Ausstattung

GPEC 2016

9. Internationale Fachmesse und Konferenz für Polizei- und Spezialausrüstung

- Rettungsgasse.jetzt
- Transport Security Technology
- Netzhärtung BOS-Digitalfunk

Interne wie externe datenschutzkonforme Polizeikorrespondenz

Der digitale Wandel von einer Industrie- zu einer Informationsgesellschaft hält auf allen sozialen Ebenen Einzug. Gerade die Etablierung von Messenger Diensten im Privatsektor beschleunigte diese Entwicklung und liefert seitdem vorteilhafte Kommunikationsfunktionen, die Angestellte, Beamte oder Führungskräfte im Unternehmen auch in ihrem Berufsalltag nicht mehr missen möchten. Die dienstliche Nutzung sozialer Netzwerke und Messenger bei Ermittlungsbehörden wie z.B. der Justiz, Polizei und Staatsanwaltschaft, wird in den einzelnen Bundesländern unterschiedlich vereinbart. Zudem ist die Zustimmung der jeweiligen Datenschutzbeauftragten, der IT-Sicherheitsbeauftragten in den jeweiligen Ländern geregelt. Eine besondere Beachtung obliegt in den Vergaberichtlinien.

Es sind jedoch geeignete Kommunikationslösungen insbesondere für Behörden notwendig und erforderlich, die den Umgang mit personenbezogenen Daten Tag für Tag gewährleisten müssen. Dabei sollte ein schneller und gesicherter Informationsaustausch zugrunde liegen.

In der Regel werden den Mitarbeiter und Mitarbeiterinnen von Behörden keine datenschutzkonformen Anwendungen bereitgestellt, sodass die Gefahr besteht, dass ggfs. die benannten Anwender aus der beruflichen Motivation heraus, ihre privaten Endgeräte sowie privaten Messenger Dienst für berufliche Zwecke verwenden, mit dem Ziel einen einsatzbedingten zeitnahen Datenaustausch innerbetrieblich durchzuführen.

Dies stellt einen dienstrechtlichen Verstoß dar und wird bei Kenntnisnahme mit disziplinarrechtlichen Maßnahmen ggfs. mit strafrechtlichen Konsequenzen geahndet. Zudem könnte ein erheblicher Imageschaden in der Öffentlichkeit die Folge sein.

Um diese zu vermeiden ist es sehr erforderlich, dass auf Entscheider Ebene, innerhalb der Ermittlungsbehörden, neben dem Verbot von unsicherem Messenger, geeignete Alternativen verwendet werden, die datenschutzkonforme Lösungen für ihre Mitarbeiter und Mitarbeiterinnen garantieren. Gut geeignet für diese Zwecke sind Anwendungen mit dem Qualitätszeichen „IT-Security made in Germany“ wie beispielsweise der Messenger Chiffry.

Dieser Messenger liefert die technische Voraussetzung für eine einheitliche Kommunikationsplattform zur einfachen und reibungslosen behördlichen Korrespondenz, intern wie extern.

Chiffry ermöglicht die abhörsichere Telefonie, den verschlüsselten Versand von Bilder, Videos, Text- und Sprachnachrichten sowie alle anderen Dokumenttypen. Der Einsatz ist ohne aufwendige administrative Tätigkeiten und

Verschlüsselungsdefinitionen möglich. Für jede Nachricht generiert Chiffry einen neuen Verschlüsselungsschlüssel und versendet diesen an den Empfänger mittels moderner 512-Bit Elliptischen-Kurven-Kryptografie. Anschließend wird die Mitteilung mit einer Ende-zu-Ende-Verschlüsselung mit 256-Bit AES im GCM-Modus codiert, an den Empfänger zugestellt und dort mit dem bereits anvertrauten Schlüssel decodiert.

Die Chiffry-Funktionen bieten Ermittlungsbehörden vorteilhafte Anwendungsmöglichkeiten. Zeugenaussagen können mit Hilfe einer Sprachnachricht aufgenommen, an die Zentrale gesendet und dort schnell bearbeitet werden. Ebenso können Dokumente wie Bilder oder Videos vom Unfall- oder Tatort zeitnah unkomprimiert in die zuständige Dienststelle versandt werden.

Mit Chiffry können Dienststellen sowie Abteilungen in Gruppen organisiert werden, die die interne Kommunikation zudem vereinfachen und fördern. Gerade bei polizeilichen Einsätzen werden Beamte über abteilungswichtige Informationen auf dem Laufenden gehalten. Dies kann ebenfalls mit Hilfe der Broadcast-Funktion erfolgen. Damit können Führungskräfte den eingesetzten Beamten, unabhängig vom Arbeitsort, eine Art Rundmail bzw. Newsletter mit internen oder externen Neuerungen zusenden. Weiterhin können Einsatzorte, Treffpunkte, Kontaktpersonen im Kollegenkreis sowie bzw. Helfende aus der Bevölkerung übermittelt werden.

In der Basis- und Premiumversionen verläuft die Kommunikation über die sich in Deutschland befindenden Server. Diese sind in einem nach ISO 27001 zertifizierten Rechenzentrum untergebracht und löschen die Nachrichten sofort nach der Zustellung oder spätestens nach 21 Tagen.

Mit der Businessversion erhalten Ermittlungsbehörden wie z.B. die Polizei eine auf ihre Bedürfnisse angepasste Lösung sowie einen eigenen Kommunikationsserver in ihrem lokalen Rechencenter. Somit verschafft sich die Polizei, die umfassende Kontrolle über die erhobenen sensiblen und personenbezogenen Daten. Es wird somit sichergestellt, dass keine Informationen bei externen Serveranbietern gespeichert oder missbräuchlich verwendet werden.

Neben der Businessversion können auch die Basis-oder Premiumversion auf einem Smartphone installiert werden. Dies ermöglicht zwei Kommunikationskreise in einen Gerät zu integrieren. Besonders geeignet für diese Zwecke sind spezielle Smartphones mit abgehärtetem Betriebssystem wie Knox oder BizzTrust. Diese Systeme ermöglichen die Einteilung des Endgerätes in einen sicheren und öffentlichen Bereich.

Somit werden nur vom Administrator definierte Anwendungen wie die Chiffry Businessversion im sicheren Bereich zugelassen. Die Premium bzw. Basisversion des Secure Messengers sowie andere Anwendungen können in dem öffentlichen Bereich installiert werden. Durch die Integration des Emoji-Sperrbildschirms mit Capture Protection wird der Zugang zum Messenger zusätzlich abgesichert.

Entwickelt wurde Chiffry von der DIGITTRADE GmbH aus Teutschenthal in Sachsen-Anhalt. Das Unternehmen ist als Hersteller von hochsicheren verschlüsselten Festplatten bekannt.

Diese sind für viele Ermittlungsbeamten, die auf dem Gebiet der Forsenik und Datenauswertung arbeiten, keine Neuheit und werden in den einzelnen Abteilungen und Organisationen gern als Backupspeicher für die datenschutzkonforme Sicherung bzw. Archivierung der Daten verwendet. Die vom ULD zertifizierte Festplatte HS256S verschlüsselt die Daten mit 256-Bit AES im CBC-Modus und bewahrt diese mit Hilfe der 2-Faktor-Authentifizierung bestehend aus Smartcard und PIN.

Dank externer Speicherung des Verschlüsselungsschlüssels auf der Smartcard eignet sich diese Festplatte sehr gut für eine sichere und kostengünstige postalische Zustellung von hochsensiblen Ermittlungsdaten an die Polizeidienststellen, Staatsanwaltschaft, Gerichte und andere Behörden.