SCHNELLER AM EINSATZORT

MOBILE

Wie funkt die Polizei?

Während Polizisten früher per analogem Funk kommunizierten, nutzen die Beamten mittlerweile zunehmend BOS-Digitalfunk. Dahinter steckt ein nicht öffentliches Mobilfunknetz, das allein von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) verwendet wird. Als technologische Basis dient das digitale Bündelfunksystem Tetra. „Das BOS-Digitalfunknetz bietet einerseits die vom Tetra-Standard vorgesehenen Sicherheitsmerkmale und andererseits spezielle vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Sicherheitsmerkmale. Im Gegensatz zu kommerziellen Mobiltelefonsystemen ist das Tetra-Digitalfunksystem daher für die Übertragung sensibler Ermittlungsdaten ebenso geeignet wie für die Übertragung personenbezogener Bürgerdaten", erklärt Olaf Kaszynski, Vorstandsmitglied des Bundesverbandes Professioneller Mobilfunk e.V. (PMeV).

Polizisten nutzen **Tetra-Funklösungen.**

als Freund UND HELFER

Mit mobilen Technologien können Einsätze von Polizei-, Rettungs- und Sicherheitskräften besser koordiniert und schneller abgeschlossen werden.

weitere Artikel

OB AUF DER AUTOBAHN, AM BAHNHOF UND FLUGHAFEN, IM RAHMEN VON GROSSVERANSTALTUNGEN ODER DER ÜBLICHEN „STREIFE“ – rund um die Uhr befinden sich in der Bundesrepublik Polizisten im Einsatz. Dabei funktioniert die Sprachkommunikationen der Beamten untereinander sowie mit der Leitstelle nach wie vor via klassischer Funkverbindungen. Zuletzt jedoch musste der bislang genutzte Analogfunk zunehmend dem neuen BOS-Digitalfunk (BOS = Behörden und Organisationen mit Sicherheitsaufgaben) weichen.

Das neue, auf dem digitalen Bündelungssystem „Tetra“ basierende Mobilfunknetz wird deutschlandweit parallel zu den kommerziellen Netzen betrieben. „Denn der Umgang mit sicherheitskritischen Daten stellt besondere Anforderungen an die Kommunikationssysteme. Abhörsicherheit, Verfügbarkeit sowie einheitliche Kommunikationsstrukturen sind hier unabdingbar“, erklärt Olaf Kaszynski, Vorstandsmitglied des Bundesverbandes Professioneller Mobilfunk e.V. (PMeV).

Das in der Einführung befindliche bzw. in vielen Bundesländern bereits genutzte digitale Tetra-Funksystem soll diese Vorgaben vollständig erfüllen. Außerdem sei es – bis zu einem gewissen Grad – für die Nutzung von Mobile-Computing-Anwendungen geeignet. „Zur Nutzung mobiler Applikationen können zertifizierte datenfähige Funkgeräte und mobile Datenterminals mit Tetra-Funktionalität eingesetzt werden“, so Olaf Kaszynski weiter. Allerdings räumt Günter Loos, ein Sprecher des Innenministeriums Baden-Württemberg, ein, dass „die Technologie nur einen relativ geringen Austausch von Daten sowie keine Nutzung von Office-Anwendungen ermöglicht.“

Ein solch rudimentärer Datenaustausch findet bei der bayerischen Landespolizei statt. „Digitalfunk dient in Bayern im Bedarfsfall zur Übermittlung von Status-, GPS- und Textmeldungen sowie zur Alarmierung vor allem der nichtpolizeilichen BOS“, berichtet der Leitende Ministerialrat Georg Ringmayr, der überdies als Leiter des Sachgebiets IC6 im Bayerischen Staatsministerium des Innern für Informations- und Kommunikationstechnik der Bayerischen Polizei zuständig ist.

iPhone & Co. kommen nicht in die Tüte

Anders als zu vermuten, nutzt die Polizei nicht nur den eigenen BOS-Funk, sondern nimmt durchaus auch die kommerziellen Mobilfunknetze in Anspruch. Für die Arbeit mit komplexen mobilen Anwendungen oder zur Übermittlung umfangreicher Dateien nutzt etwa die Bayerische Polizei seit Jahren herkömmliche 3G-Lösungen. „Dies ist aufgrund der derzeit im Vergleich zu UMTS und LTE relativ niedrigen Datenbandbreite des BOS-Digitalfunks auch künftig vorgesehen und soll weiter ausgebaut werden“, berichtet Georg Ringmayr.

Die Kanzlerin, Angela Merkel, mit einem Blackberry 10 auf der Cebit gemeinsam mit den Geschäftsführern der Secusmart GmbH, Dr. Hans-Christoph Quelle (ganz links) und dem polnischen Ministerpräsidenten Donald Tusk.

Während eine 3G-Nutzung durchaus sinnvoll sein kann, kommt der Gebrauch herkömmlicher Devices wie iPhone, Galaxy & Co. eher nicht in Betracht. „Denn handelsübliche Smartphones und Tablets sind aufgrund fehlender Tetra-Funktionalität für den polizeilichen Einsatz gänzlich ungeeignet“, so Olaf Kaszynski. Und Georg Ringmayr ergänzt: „Kommerzielle Konsumer-Tablets werden aufgrund ihrer Bauart und stark eingeschränkten Robustheit im mobilen Anwendungsbereich der Bayerischen Polizei noch nicht eingesetzt.“ Zwar ersetze man zunehmend (Bereitschafts-)Handys durch Smartphones, allerdings scheiden diese auch aufgrund der geringen Bildschirmgröße für komplexe polizeiliche Anwendungen aus. Stattdessen spielen im polizeilichen Umfeld widerstandsfähige Rugged Devices ihre Stärken aus.

Mit Bormann, Logic Instrument, Motorola oder Panasonic gibt es Anbieter, die sich auf robuste Endgeräte für den Einsatz bei Polizeibehörden und Sicherheitskräften spezialisiert haben. Dabei müssen die Devices je nach Einsatzgebiet unterschiedlichsten

Das Tablet FT03 im Einsatzwagen

SO telefoniert die Kanzlerin

Die vom Düsseldorfer Unternehmen Secusmart angebotene mobile Hochsicherheitslösung „Secusuite for Blackberry 10" wurde vom Beschaffungsamt des Bundesministerium des Inneren und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für die verschlüsselte Kommunikation der deutschen Bundesregierung ausgewählt.

Ohne Abstriche beim Nutzererlebnis soll die Lösung die sichere Verschlüsselung der gespeicherten Informationen, der Sprache, der Textnachrichten sowie des VPN bieten. Ein weiterer Pluspunkt sei das sichere Browsen, womit der gefahrlose Zugang zum Internet ermöglicht wird. Nicht zuletzt trennt die Technologie „Blackberry Balance" sensible Informationen von persönlichen Inhalten. So können Nutzer schnell und sicher zwischen ihrem geschäftlichen und privaten Leben wechseln.

www.secusmart.com

Anforderungen genügen. „Flexibilität ist extrem wichtig. Zudem sollte ein guter Spritzwasserschutz sowie Robustheit im Tagesbetrieb – also das Abfangen normaler Stöße – von den Geräten problemlos gemeistert werden", betont Armin Dußler, Leiter Vertrieb und Prokurist bei der Bormann EDV + Zubehör GmbH in Neusäß bei Augsburg.

Zugriff auf interne Systeme

Desweiteren rät Peter Damerau, Vertriebsdirektor bei Motorola Solutions Germany, bei der Auswahl auf eine IP-Schutzklassenzertifizierung zu achten. Denn diese garantiere die Widerstandsfähigkeit gegen Wasser, Staub oder außerordentliche Temperaturbedingungen. „Daneben sollten die mobilen Geräte intuitiv bedienbar und im Freihandmodus nutzbar sein, damit Einsatzkräfte schnell reaktionsfähig sind", so Damerau weiter. Über die reinen Hardware-Features hinaus spielen zudem höchste Standards beim Datenschutz eine große Rolle, wie Peter Damerau betont. Seiner Meinung nach kommt es vor allem auf die Datenverschlüsselung an, um eine sichere Übertragung sensibler Fahndungs-, Fall- oder Personendaten zu gewährleisten.

Doch die Nutzung der mobilen Devices allein bringt an sich noch wenig. Wichtig ist die nahtlose Integration bzw. Kompatibilität mit den IT-Systemen der Behörden und Leitstellen, besonders an die wichtigen Fahndungs- und Informationssysteme Polas (PolizeiAuskunftsSystem) und Inpol. Letzteres fungierte ursprünglich als Informationssystem der deutschen Landespolizeien, seit 2003 wird es jedoch als informationstechnisches Verbundsystem von Bund und Ländern genutzt. Laut Günter Loos vom Innenministerium Baden-Württemberg ist ein mobiler Zugriff auf solche Polizeisysteme unter Beachtung der Anforderungen der IT-Sicherheit und des Datenschutzes grundsätzlich möglich und auch wünschenswert, denn es könnte u.a. zu einer Reduzierung des Sprechfunkverkehrs führen.

Devices im Crashtest

Im Praxiseinsatz findet man Rugged Devices beispielweise bei der Polizei in Baden-Württemberg. „Etwa für die mobile Datenfunkanbindung an die polizeilichen Informations- und Vorgangsbearbeitungssysteme bei Kontrollmaßnahmen oder zur Vor-Ort-Auslesung von digitalen Fahrtenschreiberdaten bei LKW-Kontrollen", zählt Günter Loos auf. Denkbar wäre überdies eine Ausweitung auf die Anzeigenerfassung im Streifenwagen.

„Mobile Geräte müssen intuitiv sowie im Freihandmodus bedienbar sein, damit Einsatzkräfte schnell reaktionsfähig sind",

fordert **Peter Damerau,** Vertriebsdirektor bei Motorola Solutions Germany.

Im Freistaat Bayern hat man die Vorzüge der strapazierfähigen Geräte ebenfalls erkannt. So setzt die Bayerische Polizei seit dem Wegfall der Grenzkontrollen zu Österreich Ende der 90er-Jahre im Rahmen der Schleierfahndung mehrere hundert sogenannter Car-PC – eine Sonderentwicklung mit integriertem Monitor und Tastatur – mobil im Fahrzeug ein. „Hierüber und über die in Kürze als Nachfolger flächendeckend zur Verfügung stehenden robusten und gehärteten Car-Pads können

DEUTSCHLAND: 5,90 EUR

vor allem Abfragen in Inpol getätigt werden", so Georg Ringmayr vom Bayerischen Staatsministerium des Innern. Dadurch entfielen künftig zahlreiche Fahndungsanfragen über die Einsatzzentralen.

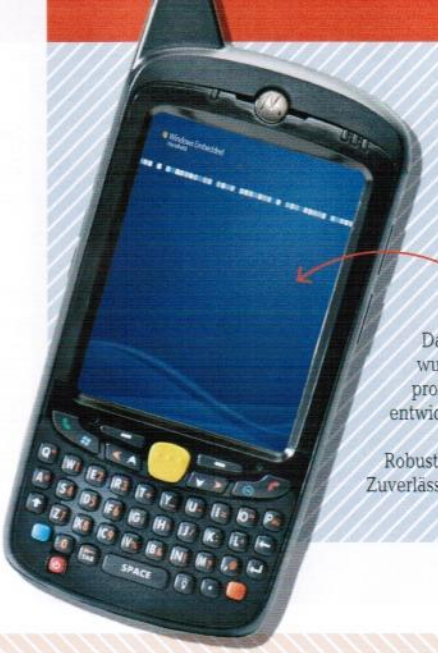
Dabei überlassen die Bayern bei der Auswahl der Hardware nichts dem Zufall. „Bei den Car-Pads ist der sichere und crashgeprüfte Betrieb während der Autofahrt wichtig", berichtet Armin Dußler von der Bormann EDV + Zubehör GmbH, die als Hardwarelieferant der Bayerischen Polizei fungiert. Desweiteren seien vor allem die Produktverfügbarkeit über mehr als drei Jahre und Wartungsverträge von bis zu zehn Jahren wichtige Kriterien bei der Device-Auswahl gewesen, ergänzt Dußler.

Nicht zuletzt verweist Peter Damerau auf ein weiteres denkbares Einsatzszenario: Bei der Aufnahme von Unfällen mussten die Einsatzkräfte früher Personen- und Unfalldaten in Papierlisten eintragen, um die Vorfälle zu dokumentieren, sowie per separater Kamera Fotos aufnehmen. Erst in einem zweiten Schritt wurden die Daten in das IT-System der Polizei eingegeben. „Dies bedeutete nicht nur einen hohen Zeitaufwand, sondern auch eine große Fehleranfälligkeit", betont Damerau. Heute können die Einsatzkräfte wichtige Daten direkt am Einsatzort abfragen, Fotos aufnehmen, Protokolldaten sofort eingeben sowie in Echtzeit an die Datenbanken der Behörde übertragen.

Das Smartphone schlägt Alarm

Neben der Polizei nutzen vor allem Rettungs- und Sicherheitskräfte mobile Lösungen während ihrer Einsätze. Zuletzt standen dabei weniger die strapazierfähige Hardware als vielmehr neue, softwarebasierte Alarmsysteme im Vordergrund. So wollen Studierende der TU Darmstadt den umgangssprachlich „Pieper" genannten Funkmelde-Empfänger von Feuerwehren und Hilfsorganisationen Konkurrenz machen: Anfang März dieses Jahres stellten sie eine „AlarmApp" für Smartphones vor, mit der die Einsatzkräfte alarmiert und gleichzeitig die Leitstellen informiert werden. „Mit der App erhalten die Einsatzkräfte den Alarm über das mobile Internet auf ihre Smartphones. Anschließend können sie per Klick die Teilnahme am Einsatz entweder bestätigen oder ablehnen. Diese Rückmeldungen werden wiederum an die Leitstelle übertragen, die damit in kürzester Zeit weiß, wer am Einsatz teilnimmt", erklärt der 25-jährige TU-Student Frank Englert, der selbst bei der Freiwilligen Feuerwehr in Kleinkahl (Bayern) aktiv ist.

Erste Anwender gibt es bereits. So nutzt die Freiwillige Feuerwehr im unterfränkischen Walda-



Das **Motorola-MC67** wurde speziell für den professionellen Einsatz entwickelt und soll hohen Anforderungen an Robustheit, Sicherheit und Zuverlässigkeit entsprechen.

FAHNDUNG PER TABLET

Dr. Gunther Guzielski, IT-Direktor des Bundeskriminalamts (BKA), gewährt im Interview einen Einblick in aktuelle Mobility-Projekte der Polizei.

Herr Dr. Guzielski, ein Großteil der polizeilichen Kommunikation wird über BOS-Digitalfunk abgewickelt – inwiefern ist vor diesem Hintergrund überhaupt die Nutzung von Mobilfunklösungen, z.B. per Smartphones und Tablet-PCs, sinnvoll?

Gunther Guzielski: Der BOS-Digitalfunk deckt einen Großteil der polizeilichen Datenkommunikation ab. Es besteht aber trotzdem zusätzlicher Bedarf an Datenkommunikation über GPRS und UMTS. Bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) können Smartphones oder Tablets den Dienstbetrieb durch den direkten Zugriff auf benötigte Informationen erleichtern. Beim Zugriff auf vertrauliche Daten müssen entsprechend sichere Produkte (VPN-Notebooks, -Smartphones) eingesetzt werden.

Wer treibt die Projekte zur Einführung mobiler Devices vor allem an?

Guzielski: Als Hauptnutzer mobiler Devices wird dieses Thema von Bundespolizei und Länderpolizeien vorangetrieben.

Welche konkreten Einsatzszenarien für Smartphones und Tablets gibt es bereits?

Guzielski: Allgemein bekannt ist die Nutzung mobiler Datenlösungen durch Polizei und Ordnungsämter insbesondere bei der Kontrolle von Verstößen und Ordnungswidrigkeiten im Straßenverkehr. Aber auch bei der mobilen Fahndung, beispielsweise in Streifenwagen, nutzen die Länderpolizeien bereits Tablets-PCs für Fahndungsabfragen, unter anderem zu KFZ-Kennzeichen oder Personendaten.

Inwieweit können Polizeibeamte im Außendienst via Smartphones und Tablets Zugriff auf Datenbanksysteme (z.B. Polas/Inpol) oder andere Backend-Systeme nehmen? Inwieweit könnten dadurch die Leitstellen entlastet werden?

Guzielski: Der Zugriff auf Datenbanksysteme via Tablet ist im Rahmen der mobilen polizeilichen Fahndung bereits möglich und entlastet so auch die Leitstellen.

Stichwort „Sicherheit": Wie können bei der Nutzung von Mobile Computing zum einen die Sicherheit sensibler Ermittlungsdaten, zum anderen der Datenschutz betroffener Bürger gewährleistet werden?

Guzielski: Die Nutzung von Mobile Computing erfordert eine zwischen der Polizei und den Datenschützern abgestimmte Sicherheits-Policy, die den rechtlichen, fachlichen und technischen Rahmen festlegt.

IS

schaff den Dienst, um die Mitglieder im Einsatzfall zusätzlich zum Pieper per App benachrichtigen zu lassen. „Dabei werden Informationen über die Anzahl der am Einsatz teilnehmenden Einsatzkräfte in Echtzeit den Gruppen- und Zugführern zur Verfügung gestellt und auf einem Rescue Information System (RIS) im Feuerwehrhaus dargestellt", beschreibt Frank Englert die Praxis. Laut Englert fragt neben Freiwilligen Feuerwehren derzeit vor allem das Technische Hilfswerk (THW) das für iOS-, Android- sowie Windows-Phone-Geräte verfügbare Alarmsystem nach. „Aktuell ist die Nutzung der App kostenlos. Da uns durch den Betrieb und die Weiterentwicklung Kosten entstehen, planen wir jedoch eine Kommerzialisierung des Dienstes", so Frank Englert. Die künftigen anfallenden Kosten hängen dann von der Größe und der Nutzungshäufigkeit des Systems ab. Laut dem TU-Student betragen diese für die meisten freiwilligen Hilfsorganisationen rund 50 Euro pro Jahr.

„Der BOS-Digitalfunk ist als Nachfolgesystem des Analogfunks das zentrale Führungs- und Einsatzmittel im polizeilichen Sprechfunk",

erklärt **Georg Ringmayr,** Leitender Ministerialrat im Bayerischen Staatsministerium des Innern.

So praktisch die Alarmierung per App ist, einen Haken hat die ganze Sache: Denn befinden sich die potentiellen Helfer in einem Funkloch, kann die Alarmierung erst zugestellt werden, wenn die Netzabdeckung wieder gewährleistet ist. Damit im Kampf um Leben und Tod keine wertvollen Minuten verlorengehen, werden Alarm-Apps klassische Systeme wie Pager und Pieper nicht vollständig ersetzen können. Und das sollen sie auch nicht, wie Frank Englert erklärt: „Pager, Pieper oder klassischer Funk können auf absehbare Zeit nicht durch die Nutzung mobiler Lösungen abgelöst werden, da diese keine Dienstgüte garantieren können. Jedoch können solch neue Informations- und Kommunikationssysteme ergänzend eingesetzt werden, um die Kommunikationswege zu verkürzen und den Informationsaustausch zu verbessern."

Einsatzplanung per Mausklick

Eine Einschätzung, die Thomas Göttgens, Geschäftsführer der Cubos Internet GmbH, teilt. Denn je „vielfältiger die Kommunikationskanäle sind, desto wahrscheinlicher ist eine erfolgreiche Alarmierung". Der in Aachen ansässige Internetdienstleister bietet mit „Group Alarm" ebenfalls ein webbasiertes Alarmierungssystem, das seit längerem über Swisscom in der Schweiz vertrieben wird und seit 2012 auch in Deutschland erhältlich ist. Mittels der Software sollen die Anwender einfach und schnell viele Teilnehmer (Mannschaft, Teams, Stäbe) alarmieren, mobilisieren oder regelmäßig informieren können. Über die Webplattform definieren die Nutzer ihre individuellen Alarmszenarien, verwalten Teilnehmer, Gruppen und Teams mit Einsatz- bzw. Rotationsplanungen und lösen per Mausklick fertige Alarme an verschiedene Empfängerkreise aus. Die Nachrichten wer-