Zukunft des Digitalfunks der BOS - Experten des AK Öffentliche Sicherheit

Positionspapier

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Marc Bachmann | Bereichsleiter Luftfahrt und Verteidigung
T 030 27576-102 | m.bachmann@bitkom.org

Verantwortliches Bitkom-Gremium

AK Öffentliche Sicherheit

Satz & Layout

Svenja Moje | Bitkom e. V.

Titelbild

© 275230 – pexels.com

Zukunft des Digitalfunks der BOS - Experten des AK Öffentliche Sicherheit

Positionspapier

Inhaltsverzeichnis

1 Einleitung

Einleitung

Im Bereich des Digitalfunks für Behörden vertritt Bitkom zahlreiche Mitglieder aus Reihen der Hersteller und Unternehmen zur Implementierung und zum Betrieb von sicherheitsrelevanten Netzen und Netzkomponenten. Im Rahmen des Arbeitskreises öffentliche Sicherheit nimmt der Bitkom deshalb gerne Stellung zu den aufgeworfenen Fragen zur Zukunft des Digitalfunks für Behörden und Organisationen mit Sicherheitsaufgaben (BOS).

2 Zukünftige Anforderungen und Dienste

2 Zukünftige Anforderungen und Dienste

Mit dem Digitalfunknetz BOS in Deutschland haben Bund und Länder eines der stabilsten Netze weltweit etabliert. Die sogenannte »einsatzkritische Sprachkommunikation« wird den Sicherheitskräften von Bund und Ländern zur Verfügung gestellt. Die bedeutendsten Kriterien für die Sicherheitskräfte sind dabei Abhörsicherheit, Schutz vor Angriffen auf interne BOS-Netze, Verfügbarkeit und Ausfallsicherheit.

Hierzu wurde die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) etabliert, die die Aufgaben von Planung bis zum Betrieb des Netzes verantwortet und im Rahmen einer gelebten und hochkomplexen Governance-Struktur die Länder- und Bundes-BOS einbindet.

Wie alle Kommunikations-Service-Provider (CSP) weltweitmüssen sich auch die behördlichen Organisationen den Herausforderungen des Marktes und dem hohen Bedarf der mobilen Zusammenarbeit stellen.

Bei der Beantwortung der Fragen in Bezug auf zukünftige Anforderungen empfiehlt es sich, die Betrachtungsebene auf den Endanwender zu konzentrieren. Diese wird oftmals vernachlässigt, obwohl hier letztendlich die Sicherheit und Ordnung produziert werden.

Generell gilt, dass die Mittel für die Kommunikation der Sicherheitskräfte sich nicht mehr von denen in der Industrie und kommerziell nutzbaren Methoden und Instrumenten unterscheiden dürfen. Unterscheiden müssen sich aber die **erforderlichen Niveaus der Vertraulichkeit, Integrität - Sicherheit und Verfügbarkeit der Dienste.**

Der zunehmende Bedarf an schneller Datenübertragung größerer Datenmengen im Einsatz ist auch in absehbarer Zeit nicht durch TETRA-Geräte und –Infrastruktur zu decken. Kommerzielle Tablets und Smartphones mit LTE-Anbindung bilden hier eine **sinnvolle komplementäre Ergänzung.** Diese handelsüblichen Geräte sind als BSI-zugelassene Endgeräte (VS-NfD) erhältlich, bieten ein vergleichbares Schutzniveau und bauen auf marktübliche Akzeptanz bei der Bedienerfreundlichkeit moderner Endgeräte.

Für ein behördliches Sprachnetz bzw. kombiniertes Sprach- und Datennetz stellt sich die grundlegende Frage, ob TETRA ab 2025 noch die Technologie bleiben wird, die die klassische Sprachübertragung (hauptsächlich gruppenorientiert) der BOS-Organisationen in Deutschland und Europa bereitstellt. Vieles spricht dafür, denn derzeit ist noch keine ähnlich ausgereifte Technologie verfügbar, die die Kernanforderungen an auch in Krisensituationen verfügbaren für BOS Einsatzkräfte unabdingbaren Sprachleistungsmerkmalen wie Gruppenrufe, Rufpriorisierung, dynamische Gruppenbildung etc. erfüllen könnte.

Unabhängig von dieser Technologiefrage bleiben die hohen Sicherheits- und Verfügbarkeitsanforderungen an ein behördliches Sprachnetz bzw. an ein kombiniertes Sprach- und Datennetz weiterhin bestehen. Ein zukünftiges BOS Sprach- und Datennetz muss die Sicherheitsanforde-

rungen erfüllen, die auch heute schon im BOS Digitalfunknetz erfüllt werden. Es ist nicht abzusehen, dass ab 2025 die Bedrohungs- und Risikosituation im BOS-Digitalfunk als weniger hoch eingeschätzt wird. Eher wird das Gegenteil der Fall sein.

Bei den über Funk übermittelten Daten handelt es sich um vertrauliche Daten (polizeilich relevante Daten), die gemäß VSA (Verschlusssachenanweisung) in besonderer Weise zu schützen sind. Sofern das zukünftige BOS Digitalfunknetz als »Kritische Infrastruktur« im Sinne des Gesetzgebers zu betrachten ist, ergeben sich darüber hinaus noch zusätzliche Anforderungen an die Sicherheitsinfrastruktur des Netzwerks, um Angriffe erkennen, abwehren und melden zu können. Zu einem weiteren Aspekt, den Security Operation Center (SOC), folgen unten weitere Ausführungen.

Die Anforderungen an die Verfügbarkeit (99,95 %) des missionskritischen Anteils des BOS Digitalfunknetzes werden daher auch in Zukunft bestehen bleiben. Daraus kann gefolgert werden, dass die derzeitigen Vorsorgemaßnahmen bei der Energieversorgung auch in Zukunft mindestens auf gleichem Niveau bestehen bleiben müssen. Dies gilt auch für die hochverfügbare Auslegung des BOS Kernnetzes sowie für die strikte sicherheitstechnische Trennung und Entkopplung dieses Netzes von anderen Netzen.

In einem zukünftigen BOS Digitalfunk können jedoch infolge der Verfügbarkeit von breitbandigen Funkdatendiensten neben der Sprache und sonstigen Diensten (wie z. B. Kurznachrichten) weitaus größere Datenmengen über die Luftschnittstelle von und zu den BOS-Endgeräten übertragen werden. Solche breitbandigen Verbindungen können für viele wichtige neue Anwendungsszenarien genutzt werden, die im heutigen Digitalfunk nicht möglich sind.

Aspekte der uneingeschränkten »Hoheit« über das Netz für die BOS im Krisenfall

2.1. Anforderungen von heute und Übermorgen

Die derzeitigen BOS Netze sind mit einem besonderen Anforderungsprofil geschaffen worden und stellen entsprechend ihren Anforderungen für die Sprachdienste Leistungen zur Verfügung. Der Prozess von den formulierten Anforderungen bis zur Umsetzung hat jedoch mehr als eine Dekade gedauert. Die erste Ausschreibung des Innenministeriums zum Digitalfunk der BOS lag beispielsweise zwei Jahre vor der breiten Einführung von Smartphones. Die Technologien haben sich unterdessen rasant weiter entwickelt und auch die BOS müssen sich der Lage anpassen.

Dies betrifft z. B. folgende Anforderungen, die auch schon heute teilweise erforderlich sind:

- die Übertragung von Video- oder Bilddaten, Lagebilder,
- die Nachrichtenbasierte Kommunikation (z. B. E-Mail, SMS, Messenger, ...) zwischen Einsatzkräften der BOS
- Online-Abfrage von Daten bei den BOS-Organisationen, wie Polizei, Feuerwehr und den Rettungsdiensten mit den hochmobilen BOS-Endgeräten,
- die Softwareaktualisierung der BOS-Endgeräte (over the air)

Einerseits ergeben sich mit diesen Erweiterungen erhebliche Mehrwerte für den BOS Digitalfunk, auf der anderen Seite erhöht sich dadurch auch die Bedrohungssituation. Die derzeit eingesetzte Ende-zu-Ende Verschlüsselung ermöglicht zwar die Verschlüsselung von Sprache und Kurznachrichten, jedoch nicht die Verschlüsselung von Daten (z. B. E-Mails), die über das IP-Protokoll ausgetauscht werden.

In einem zukünftigen BOS-Digitaldatenfunknetz müssen daher zusätzliche Sicherheitsmaßnahmen umgesetzt werden. Dies betrifft z. B.

- eine Ende-zu-Ende Verschlüsselung (VS-konform) von über das IP-Protokoll transportierten Daten zwischen den Endgeräten zur Leitstellen und
- eine Verschlüsselung (VS-Konform) von auf den Geräten gespeicherten Daten.

Darüber hinaus müssen in einem zukünftigen behördlichen oder einem kommerziellen BOS Sprach- und Datennetz folgende grundlegende Sicherheitsanforderungen umgesetzt werden:

- Hochverfügbarkeit in Krisensituationen
- VS-konforme Ende-zu-Ende Verschlüsselung von Sprache zwischen allen Teilnehmern
- Funktionen zur Erkennung und Abwehr von gezielten Angriffen auf kritische Infrastrukturen im BOS Kernnetz
- VS-konforme Verschlüsselung von Steuerdaten, Managementdaten und Verkehrsdaten im Netz
- Sicherheitstechnische Trennung der unterschiedlichen Teilnetzbereiche und Netzabschnitte im BOS Kernnetz
- Redundante Standort-Infrastrukturen
- Hochverfügbar und hochredundant ausgelegtes BOS Kernnetz (Leitungen, Systeme)
- Sicherheitsüberprüftes Betriebspersonal Hoheit über Netz / Netzbetrieb im Krisenfall

Die weiter ausdifferenzierten Anforderungen und Profile des künftigen Digitalfunks aus Sicht der Bitkom Unternehmensexperten sind am Ende des Papiers ausführlich zusammengefasst.

2.2. Trendaussagen für den weiteren Ausbau des BOS Digitalfunks

- Moderne Endgeräte erlauben eine intuitive Bedienbarkeit und steigern die **Attraktivität des Arbeitsplatzes** der Sicherheitskräfte. Arbeitsweisen, ob im Einsatz, in der Dienststelle oder privat verschmelzen langfristig. Die sichere dienstliche und sonstige Nutzung mobiler Endgeräte wird auch in den Sicherheitsbehörden Einzug halten (Endgeräte-Management MDM erforderlich). Sicherheitskonzepte erlauben eine saubere Trennung zwischen privatem und hochsicherem Gebrauch. Durch die ergänzende Nutzung handelsüblicher Endgeräte lassen sich die Endgeräte-Kosten nachhaltig minimieren und den Sicherheitskräften stehen modernste Technologien zur Verfügung, die dem Stand der Technik entsprechen.

- Der Einsatz von autark aufgesetzten mobilen Netzen oder auch nur von ergänzenden mobilen Basisstationen, gibt den BOS in Großschadenslagen oder bei Großereignissen, wie dem G8 Gipfel in Elmau, die nötige Flexibilität, um auch in abgelegenen Regionen stets sicheren Breitband Digitalfunk zur Verfügung zu haben. Diese Mobilen Digitalfunkanlagen können in LKW zum Einsatzort gebracht werden und dort für die Einsatzdauer zur Verfügung stehen. Ein entsprechender Netzausbau für Spitzenlasten, die wie in Elmau vielleicht nur ein einziges Mal gebraucht werden, ist vergleichsweise ineffizient.

- Kommunikations- und Datendienste werden unabhängig von den Bauformen durch einen **BOS Digital Service Provider (DSP)** über einen BOS-App-Store deutschlandweit nach Zielgruppen (Feuerwehr, Polizei, Rettungsdienst, Katastrophenschutz etc.) geprüft, zugelassen und bereitgestellt. Das bedeutet nicht zwangsläufig, dass auch die Services durch den Service Provider entwickelt werden. Die dislozierten Fachabteilungen der Ressorts in Bund und Ländern entwickeln arbeitsteilig neue Apps und übergeben sie in den BOS-App-Store zur sofortigen Nutzung. Einsatz-Know-how und Erfahrungen werden wertschöpfend für alle verfügbar gemacht. Der Abstimmungsaufwand wird sich durch diese Rollenschärfung deutlich minimieren.

- Die Kommunikationsnetze basieren umfänglich auf den aktuellen IP-Standards und verschmelzen zunehmend in einem hybriden Gesamtnetz, welches den notwendigen Austausch behördenübergreifend und für gewisse Aufgaben auch grenzüberschreitend unterstützt. Über definierte Schnittstellen (Application Programming Interfaces/API) erfolgt die Konvertierung von Protokollen und Formaten zum Datenaustausch. Das bedeutet auch, dass einsatzkritische Sprachverbindungen zunehmend mehr und sicher durch Parallelnetze übertragen werden und nur im Ernstfall, bei Zusammenbruch priorisierter Breitbandnetze, ausschließlich durch das TETRA-Netz. Die Verfügbarkeit des Notfallnetzes bei Stromausfall muss deutschlandweit über 72 Stunden gewährleistet sein und periodisch getestet werden.

- Hintergrundauswertungen analysieren Situationen und den aktuellen Status in Echtzeit und geben **automatisiert taktische Unterstützung, Entscheidungshilfen und -vorschläge**, angepasst auf aktuelle Einsatzsituationen. Hierzu sind **kognitive Technologien** zwingend notwendig, die u.a. bei der Zusammenführung bestehender Insellösungen helfen. Damit können bestehende individuelle Ausprägungen und bestehende Abhängigkeiten von Leitstellen- und Kommunikationsanbietern an- bzw. ausgeglichen werden. Das hat zur Folge, dass die fachliche Vernetzung mit Blick auf übergreifende Lagezentren für effiziente Entscheidungsprozesse erfolgen kann / ermöglicht wird. Die Einbindung von Bürgerhinweisen und die Auswertung sozialer Netzwerke sind unabhängig von Inhalten möglich, können aber durchaus in ein Gesamtlagebild einfließen.

- Alle Endgeräte wählen automatisch das für die jeweilige Aufgabe bestgeeignete Netz. Mit einem **automatisierten Endgeräte-Management** aktualisieren sich die Endgeräte in den Dienststellen (oder andere Orte mit hoher Netzbandbreite) selbstständig (bspw. Patchen über das Netz) und benötigen somit kaum noch ein manuelles Eingreifen. Damit ist stets das höchste Sicherheitsniveau gegeben und Gruppen können dynamisch aktualisiert werden. Dazu notwendige Services werden automatisiert als Webservices bereitgestellt (Nutzereigenes Management (NeM & NMC) etc.).

2.3. Bitratenanforderungen für zukünftige Dienste in einem behördlichen Sprachnetz bzw. einem kombinierten Sprach- und Datennetz

Die konkreten Bitratenanforderungen zu formulieren, ist angesichts der planungstechnischen Vorlaufzeiten schwierig. Es müsste aufgrund unklarer technischer Entwicklungen auf Bandbreiten hochgerechnet und vorhergesagt werden, welche Dienste wann und wo bereitgestellt werden müssten. Wenn man sich dann insbesondere die Unterscheidung zwischen Mission Critical und Best-Effort Diensten für einen Zeitrahmen bis 2030 vor Augen führt, wird die hohe Anzahl unkalkulierbarer Variablen sichtbar.

Die Bandbreiten im mobilen Datenfunk haben sich die letzten Jahre rasant entwickelt. Fast alle Unternehmen nutzen diese Möglichkeiten und statten die mobil im Einsatz befindlichen Mitarbeiter zur Produktivitätssteigerung mit entsprechenden Lösungen aus. Damit einhergehend werden die Geschäftsprozesse auf mobile Arbeitsweisen angepasst und umgestellt. Eine wichtige Einflussgröße ist die Bandbreite des verfügbaren Netzes, welche sich regional stark unterscheidet.

Hier prägen sich zwei Arbeitsweisen aus, welche durch die angebotenen Mobilen Lösungen unterstützt werden. Während in der überwiegenden Zahl der Fälle eine ausreichende Netzanbindung zur Verfügung steht, so ist insbesondere in den Fällen mit fehlender Abdeckung eine Offline-Fähigkeit von Anwendungen notwendig, die zusätzlich durch eine Not-Kommunikation im Falle der Sicherheitsbehörden unterstützt werden muss.

An diesem Beispiel zeigt sich die Tragweite der Entscheidung der Bundesregierung, mit der Investition in das TETRA-Netz die deutschlandweite, für erfolgreiche Einsätze der Sicherheitskräfte kritische und hochverfügbare Kommunikation parallel zu den klassischen Mobilfunkanbietern bereitgestellt zu haben.

Für die mobilen BOS Einsatzszenarien sollte die Bandbreite des mobilen Datenfunks keinesfalls hinter den marktüblichen Standards zurückliegen. Ob die in der Fachwelt angedachten Frequenzbänder diesen Bandbreiten genügen und ob deren Umsetzung eine akzeptable Kosten-Nutzen-Relation ergibt, bedarf weiterer tiefergehender Analysen. Hier ist insbesondere der für internationale und nationale Frequenzregulierung anzusetzende Zeitbedarf für die schnelle Weiterentwicklung der Infrastruktur kritisch.

Erfahrungsgemäß folgen die möglichen Arbeitsweisen den verfügbaren Bandbreiten. Ca. 75% der Bandbreite wird nach Expertenmeinungen durch die Nutzung von Videoinhalten beansprucht. Einsatzszenarien für Körperkameras bei Einsatzkräften werden bereits heute getestet. Sie erhöhen die Sicherheit der Einsatzkräfte und benötigen für eine Echtzeit-Situationserkennung entsprechende Übertragungskapazitäten.

Zu den konkreten Bedarfen gibt es bereits zwei entsprechende Studien, die für das BMI erstellt wurden.

3 Architektur und Technologieoptionen

3 Architektur und Technologie-optionen

Im folgenden Abschnitt werden die derzeitigen Technologiestandards in den Blick genommen und deren Überführung in eine zukunftsfähige Digitalfunklösung der BOS ohne das Rad neu zu erfinden.

3.1. Weiterentwicklungen des TETRA Standards bis 2025?

Unter den derzeitigen Voraussetzungen erscheint es eher unwahrscheinlich, dass sich Leistungsmerkmale in TETRA wesentlich ändern bzw. wesentliche Leistungsmerkmale neu hinzukommen werden. Die namhaften TETRA-Hersteller gehen bereits den Weg, ihre Systeme mit LTE zu koppeln bzw. eigene LTE-Lösungen zu entwickeln und Migrationspfade hin zu LTE aufzuzeigen (z. B. Einsatz von Software Defined Radios, TETRA-Apps auf Smartphones etc.).

Die Fortschreibung der heute existierenden TETRA Standardisierung liegt in den Händen des ETSI TCCE (TETRA and Critical Communication Evolution) Komitees. Gemäß Jahresbericht 2015 wird der Fokus bei der Weiterentwicklung auf der Ergänzung um Breitbandfähigkeiten liegen. Hauptproblem hierbei ist der Bedarf an zusätzlichen Frequenzspektren, für deren Bereitstellung bereits mit den europäischen Regulierungsbehörden zusammengearbeitet wird. Dabei werden Methoden zur Integration von TETRA in Breitbandlösungen betrachtet und die Möglichkeit der Migration des (zukünftigen) TETRA zu einer Breitbandlösung.

In Anbetracht der sichtbaren Defizite der aktuellen TETRA-Standardisierung im Bereich Daten-Breitbandkommunikation ist bis zur Verabschiedung entsprechend überarbeiteter Standards zu erwarten, dass auch konvergente bzw. Hybridlösungen für die Adressierung der Nutzerbedarfe als Lösung herangezogen werden müssen, um den gesellschaftlichen Anforderungen an öffentliche Sicherheit gerecht zu werden. Die zunehmende Konvergenz verschiedenster Netzinfrastrukturen (z. B. Mobilfunk, Kabel, WLAN etc.) wird als Trend auch im Bereich kommerzieller Netzbetreiber beobachtet.

Hier spielt die Virtualisierung bestimmter Netzfunktionen (Network Function Virtualization/ NFV) als weiteres Thema der Standardisierung innerhalb des ETSI eine große Rolle, da sie für die Kopplung und Integration verschiedener Netze die Voraussetzungen schafft. In die gleiche Richtung bewegt sich Software Defined Networking (SDN). SDN ist die Voraussetzung für den wirtschaftlichen Betrieb flexibler Kommunikationsnetze, da mit SDN die Kontrollfunktionen von den Datentransportfunktionen entkoppelt werden und auch in komplexen Szenarien handhabbar bleiben. Auf diesem Weg ist die enge Integration von Netzwerken mit den benötigten Fachanwendungen auch unter den künftigen Bedingungen eines hochflexiblen und agilen, voll digitalisierten Ökosystems aus Betreibern, Herstellern und Anwendern durch die Nutzung von Cloud-Technologien realisierbar.

Der Einsatz bzw. das Einführen von TETRA 2 (TETRA Enhanced Data Service, TEDS) für die deutsche BOS wird generell skeptisch gesehen, da mit TEDS ebenfalls nur vergleichsweise niedrige Datenraten (bis zu einigen hundert kbit/s) zur Verfügung stehen und bereits jetzt der Frequenzbereich für das deutsche BOS-TETRA-Netz vollkommen ausgeschöpft wird (Frequenzen für die Einführung von TEDS stehen derzeit nicht zur Verfügung).

3.2. Technologiealternativen oder Erweiterungen zu TETRA für ein behördliches Sprachnetz bzw. ein kombiniertes Sprach- und Datennetz

Als realistische, mindestens **mittelfristige** Alternative wird ein hybrides Netz, bestehend aus einem TETRA-Teilnetz für »mission critical« Sprach- und Datendienste (Einzelruf, Gruppenruf, Rufpriorisierung, SDS) und ein exklusiv für die BOS zur Verfügung stehendes LTE-Netz zur hochbitratigen Datenübertragung (u.a. auch Video) gesehen.

Eine wesentliche technische Alternative in einem zukünftigen kombinierten Sprach- und Datennetz stellt die Verfügbarkeit von LTE dar, in dem es möglich ist, 300 Megabit pro Sekunde oder mehr zwischen den Endgeräten über Funk zu übertragen.

LTE könnte über eine LTE-Basisstation eines Mobilfunknetzes für die IP-Kommunikation zum BOS-Kernnetz genutzt werden. Neben TETRA müssten die BOS-Endgeräte dazu auch LTE unterstützen. Zur Verschlüsselung und Authentisierung von IP-Kommunikation kann z. B. der Standard IPSec verwendet werden. VS-konforme Verschlüsselungsfunktionen auf Basis dieses Standards sind am Markt verfügbar, allerdings noch nicht auf den derzeitigen BOS-Endgeräten. Hierzu muss frühzeitig eine entsprechende Entwicklung bei möglichen Herstellern angestoßen werden, damit eine solche Technologie rechtzeitig ausgereift am Markt verfügbar sein kann.

Für die Umsetzung einer VS-konformen Ende-zu-Ende Verschlüsselung über IP muss ein sicherer Schlüsselspeicher auf der Seite der BOS-Endgeräte und der Leitstellen bestehen. Ein sicherer Schlüsselspeicher kann z. B. eine Smartcard im micro SIM-Card-Format sein, die in das BOS-Endgerät eingesteckt wird. Auf der Seite der Leitstellen kämen für Verschlusssachen vom BSI zugelassene Standard-Verschlüsselungssysteme in Frage.

Damit die Endgeräte eine IP-Verbindung zu den Leitstellen der BOS-Organisationen aufnehmen können, müssten Übergänge aus dem LTE-Netz zum BOS Kernnetz geschaffen werden. An das BOS Kernnetz sind die Kommunikationspartner der BOS-Organisationen bereits angeschlossen. Auswirkungen auf das BOS Kernnetz hätte dieser Übergang »nur« in der Weise, dass das BOS Kernnetz von der nutzbaren Bandbreite her in der Lage sein müsste, die zusätzliche Datenkommunikation aus dem LTE-Netz mit aufzunehmen.

Dies wird dazu führen, dass im BOS Kernnetz in Zukunft deutschlandweit größere Mengen an Daten übertragen werden müssten als bisher, sodass das BOS Kernnetz wesentlich höhere

Übertragungsbandbreiten unterstützen müsste. Darüber hinaus müsste das Kernnetz auch erweitert werden, da auch an mehr Anschlussstellen kommuniziert werden muss.

Unter der Prämisse der Nutzung standardisierter Netze, speziell LTE, stellen marktgängige Endgeräte (Tablets & Smartphones) eine sinnvolle und in jeder Hinsicht vorteilhafte Ergänzung zum TETRA Standard dar.

Speziell für die komplementäre Aufgabe der sicheren Datenübertragung weisen diese Endgeräte massive Vorteile gegenüber TETRA Geräten auf:

- hohe Datenübertragungsraten
- einfache & gewohnte Handhabung (nutzerfreundlich)
- direktes Partizipieren am technischen Fortschritt durch Nutzung handelsüblicher Geräte mit hohen Stückzahlen
- hoher Reifegrad der Endgeräte
- ausgefeilte Update- (OTA Updates der Gerätehersteller oder Netzbetreiber) und Managementfunktionen (Mobile Device Management)
- Programmierschnittstellen mit extrem hohem Verbreitungsgrad (Unterstützungspotenzial)
- taktisch: Visuelle Unauffälligkeit beim Gebrauch im Einsatz gegenüber BOS Geräten
- Reduktion der Anzahl der mitgeführten Geräte
- Durch Nutzung gleicher Sicherheitskomponenten (BOS SKE-Karte) bleibt das Schutzniveau voll erhalten.

Um marktgängige Endgeräte sicher nutzen zu können, muss eine adäquate Infrastruktur aufgebaut werden. Dazu gehören u.a. VPN-Gateway, ein API Management, Mobile Device Management, Security Incident Event Management (SIEM) sowie Mobile Application Management. Diese Komponenten sind elementare Bestandteile der BSI-konformen Gesamtarchitektur und dienen einer konsistenten Steuerung und Kontrolle der zu betreibenden Netz- und Anwendungsinfrastruktur.

Langfristig ist abzuwarten, ob LTE mit den Leistungsmerkmalen für den »Mission Critical«-Einsatz (Release 13 und 14) alle derzeit diesbezüglich von BOS genutzten Dienste abbilden kann und vor allem, wann es die entsprechende Systemtechnik und die Endgeräte hierfür in Deutschland gibt.

Für die Integration z. B. von LTE-Geräten sind weiterhin Gateways zwischen den beiden Infrastrukturen (BDBOS- und LTE-Netz) zum Einsatz erforderlich, die den Datenstrom eines Netzes für den Weitertransport im jeweils anderen Netz umformen. Diese sind heute als herstellerspezifische Lösungen bereits verfügbar. Über Apps werden die Bedienfunktionen der TETRA-Gerätetechnik nachgebildet, so dass ein einfacher Wechsel zwischen den Gerätefamilien möglich ist.

Ebenso ist die Nutzung des LTE-Backbones für TETRA-Basisstationen durch entsprechende Fähigkeiten der Basisstationen möglich. Ziel muss es jedoch sein, herstellerspezifische Lösungen zu vermeiden und standardisierte Netzübergänge zu realisieren.

Die Mitbenutzung **öffentlicher** Netze bietet sowohl Chancen als auch Risiken. So wären evtl. durch Verbindungen aus dem öffentlichen Netz Angriffe auf das Digitalfunknetz möglich. Um solche Angriffe frühzeitig zu erkennen und in Echtzeit zu reagieren ist ein sogenanntes **Security Operation Center (SOC)** notwendig.

Ein SOC umfasst grundsätzlich mehrere Komponenten und stellt somit eine Plattform dar, die als Kommandozentrale für Cyber Security gesehen werden kann. Hier laufen alle relevanten Informationen aus der IT-Umgebung und dem Netzwerk zusammen und werden korreliert analysiert. Beispielsweise stehen den Analysten verschiedene Dashboards zur Verfügung, die diverse Vorgänge im hybriden Netzwerk und der IT-Umgebung darstellen. Diese können dann in unterschiedlicher Granularität angezeigt werden. Bei auffälligem Verhalten werden Alarme generiert, welche daraufhin forensisch durch Analyse- und Reportwerkzeuge weiter untersucht werden können.

Dies ermöglicht es den **Emergency Response Teams der BDBOS**, ein aktuelles Lagebild der derzeitigen IT-Sicherheit im übergreifenden Netzwerk zu erzeugen. Damit ist die Darstellung und Beurteilung der aktuellen Cyberbedrohungslage gemeint, sowie die Fähigkeit zur Reaktion bei IT-Sicherheitsvorkommnissen, beziehungsweise zur Wiederherstellung der IT-Cybersicherheit nach einem Vorfall.

Um diese Anforderungen zu erfüllen, sowie der Gründung eines SOCs gerecht zu werden, bedarf es einer guten **Security Incident- und Event-Management Lösung (SIEM)**, die alle relevanten Informationen aus der IT-Umgebung zusammenführt. Ein SIEM konsolidiert Ereignisdaten aus Protokollquellen von tausenden Endpunkten und Anwendungen im gesamten Netz. Es führt sofortige Normalisierungs- und Korrelationsaktivitäten der Rohdaten aus, um echte Bedrohungen von vermeintlichen (sogenannte »False Positives«) zu unterscheiden.

Somit kann innerhalb kürzester Zeit ein kompetentes Lagebild der IT- sowie Netz-Infrastruktur erzeugt werden und die Emergency Response Teams können jederzeit schnell und effektiv handeln. Ein weiterer, enormer Mehrwert entsteht für ein SOC durch eine sogenannte **Daten-Fluss-Analyse (Flow Analyse)**. Ein Angreifer hinterlässt in der Regel Spuren in Log-Dateien. Diese Spuren kann er am Ende der Attacke einfach verwischen oder vernichten, indem er die Logeinträge fälscht oder diese sogar löscht. Dies ist bei einer Datenflussanalyse in Echtzeit nicht möglich. Bei einer Daten-Flow-Analyse kann man bis zum OSI Layer 4 alle Informationen eines Datenpaketes im Netzwerk einsehen.

3.3. Realistische / wirtschaftliche Architekturszenarien

Die Wünsche aus dem Dienstalltag treffen immer wieder auf die Schranken der Realität. Deshalb soll auch dargestellt werden, welche Szenarien (z. B. dediziertes [Rumpf-]Netz, Mitnutzung öffentlicher Netze, Mischszenarien) unter Nutzung der TETRA Technologie und der in Aussicht gestellten Breitbandfrequenzen zur Realisierung von Sprach- und Datendienste für die BOS in Deutschland realistisch und wirtschaftlich sind. Dazu zunächst in kurzen Stichpunkten das Wesentliche:

- Weiternutzung des derzeitigen TETRA-Systems für »mission critical« Sprach- und Datendienste (Einzelruf, Gruppenruf, Rufpriorisierung, SDS).
- Ein zusätzlich für die BOS exklusives und anforderungsgerechtes (siehe unten) LTE-System für breitbandige Datenanwendungen. Dabei sollten Breitbanddienste bedarfsgerecht und schrittweise eingeführt werden. Hierzu ist es zunächst notwendig, mit BOS-Nutzern Anforderungen zu analysieren, dann bedarfsgerechte Applikationen zu entwickeln und diese anschließend mit den Nutzern zu testen und einzuführen.
- Ergänzende Nutzung von öffentlichen mobilen Breitbandnetzen unter Gewährleistung der erforderlichen IT-Sicherheit für niedrig priorisierte »non mission critical« Anwendungen.

Der **Digitale Service Provider (DSP)** stellt den Endkunden und dem gesamten zukünftigen BOS-Ökosystem seine Services mehrheitlich digital zur Verfügung. Der DSP konzentriert sich wesentlich auf die Zufriedenheit der Endnutzer bzgl. der optimalen (taktischen) Unterstützung ihrer Arbeit. Es nutzt verstärkt analytische Fähigkeiten, um zu verstehen, was in seinem hybriden Netzwerk inklusive angeschlossener Servicezentren in Echtzeit vor sich geht, um neue automatisierte Services anzupassen. Sicherheit und Zuverlässigkeit, sowie hohe Flexibilität, sind dabei die Haupterfolgskriterien. Aus heutiger Sicht sollte die BDBOS bzw. der Betreiber oder ein für das Netz verantwortlicher Generalunternehmer diese Rolle annehmen und ausfüllen.

Der **Digitale Service Enabler (DSE)** entwickelt neue digitale Services und stellt sie über den DSP dem Ökosystem zur Verfügung. Beispielsweise entwickelt die Bundespolizei eine Anwendung zum polizeilichen Messaging. Oder der Endgerätehersteller stellt automatische Sicherheits-Patches (?) für die Endnutzer bereit. Diese Services werden dem Ökosystem zur Nutzung über den Serviceprovider zur Verfügung gestellt, damit in Großlagen behördenübergreifend kommuniziert werden kann. Hierzu ist eine Öffnung der Services des DSP mittels standardisierter Schnittstellen (APIs) wie z. B. Web Services (im Sinne einer serviceorientierten Architektur, SOA) notwendig. Ggf. müssen bestehende APIs in vorhandenen Anwendungen geeignet transformiert werden, um eine Anbindung von Partnern im Ökosystem zu realisieren.

3.4. Innovationsentwicklung bei den Endgeräten

Es stellt sich natürlich die Frage, welche Innovationen bei der Entwicklung neuer Generationen von Endgeräten wann zu erwarten sind. Beispiele für diese Innovationen wären Mehrfrequenztauglichkeit, Unterstützung mehrerer Technologien, »Dual«-BOS-Sicherheitskarte, Integration der BOS-Sicherheitskarte (eSIM) in Gerätesoftware, Datenservices etc.

Duale Geräte TETRA / LTE sind in der Entwicklung. Viele der zu erwartenden Veränderungen im Bereich der mobilen Endgeräte wurden bereits in der Fragestellung benannt. Speziell Mobilgeräte von führenden Anbietern bieten bereits mit der sog. Trustzone hier eine HW-Architektur, die grundsätzlich die sichere Ablage von Kryptomaterial ohne Zusatz-Hardware ermöglicht (eSIM/ Soft SIM).

Bereits heute wird die Trustzone für BSI—zugelassene Mechanismen des Trusted- & Secure Boot genutzt, eine Erweiterung auf die Ablage von Schlüsselmaterial ist möglich.

Perspektivisch wird die Verwendung von abgeleiteten, an mobile Endgeräte gebundenen Credentials und Schlüsselmaterialien, sowie die zusätzliche Nutzung von biometrischen Online-Identifizierungs- und Authentisierungsmechanismen zusätzliche Sicherheitsfunktionen bieten. Damit wird eine hochsichere Systemlösung mit einer effizienten Administration der Endgeräte ermöglicht.

Die Eliminierung des Einsatzes spezialisierter Hardware ist ein Trend, der dem Bedarf der flexiblen und schnellen Anpassung der genutzten Technik an die Nutzerbedürfnisse Rechnung trägt und auch weltweit zu beobachten ist.

Die Echtzeitauswertung aller verfügbaren Informationen im Einsatzfall kann nicht nur das Leben Betroffener, sondern auch das der Einsatzkräfte retten. Kognitive Systeme können diese Daten subsummieren, verstehen und Ratschläge für spezielles Verhalten geben. Das Selbstlernverhalten garantiert, dass die Ratschläge ständig besser werden und aus Fehlern gelernt wird. Diese kognitiven Systeme und Technologien unterstützen bei der Entscheidungsfindung – sie können evidenzbasierte Handlungsoptionen vorschlagen. Dabei passen sich diese Optionen kontinuierlich, beinahe in Echtzeit, an neue Wissensstände an. Schon heute werden diese Technologien von Callcentern in Stresssituationen genutzt, oder auch zur Anamnese bei schwersten Erkrankungen.

Vor dem Hintergrund des demografischen Wandels sowie des Mangels an Ressourcen (auch im Sicherheitsbereich), werden vorausschauende Arbeitsweisen immer bedeutsamer. Sie wirken sich auf die gesamte Disponierung der mobilen Einsatzkräfte aus und können bspw. proaktiv Stausituationen antizipieren. Ziel ist dabei, die Prozesse mit geringer menschlicher Einwirkung zu durchlaufen, um Fehlerpotenzial zu minimieren und Verzögerungen im Ablauf zu reduzieren.

Self-Service und die Einbindung sozialer Netzwerke zeigen in der heutigen BOS Landschaft, wie sich Anwendergruppen zur Zufriedenheit, zu Wartungsproblemen oder über Tipps und Tricks austauschen. Dieser Trend wird nicht nur in der Behördenwelt, sondern auch massiv in der Wirtschaft genutzt und stärkt die Rolle des Endnutzers. Mit praktischen APPs wird bereits heute die kritische Einsatzkommunikation angereichert. Deren Ausbreitungsgeschwindigkeit ist weiter als hoch zu bewerten.

Das Internet der Dinge wird auch die Sicherheitsbehörden im Einsatz beeinflussen. Schon heute wird die mobile Kommunikation in einem interaktiven Streifenwagen mit Funktionen des Einsatzfahrzeuges zusammengeführt. Dieser Trend wird sich weiter verstärken und die mobilen Einsatzfahrzeuge werden intelligente Kommunikationsservices bereitstellen.

Mit der zu erwartenden breitbandigen Datenkommunikation bis zum Endgerät wird sich dieses zu einem universellen Kommunikationshub verändern. Technologien wie RFID, NFC, Bluetooth, IP, Geo Location Services, Kameras, Internet of Things, Analytics, Cognitive werden im Endgerät verfügbar und genutzt, um jederzeit z. B. die Vollständigkeit der Ausrüstung zu gewährleisten, die Situation besser einzuschätzen die erweiterte Führungsmöglichkeiten für die Einsatzführung der Zukunft zu nutzen.

4 Eignung kommerzieller Netze für die behördliche Nutzung

4 Eignung kommerzieller Netze für die behördliche Nutzung

Die vorherigen Abschnitte haben gezeigt, dass eine ökonomisch sinnvolle und dennoch der Dynamik aktueller Entwicklungen angepasste Lösung nur durch Einbindung und Nutzung von Synergien mit bestehenden Netzinfrastrukturen möglich ist, um mittelfristig eine anforderungsgerechte und zeitgemäße Funklösung für die BOS zu realisieren. Im folgenden Abschnitt wird beschrieben, was nötig ist, diese Synergien der Netze herzustellen.

4.1. Situation der kommerziellen Netze in Deutschland und der benötigte Anpassungsbedarf

Der LTE Standard ist derzeit nicht für die Verwendung als Basistechnologie für kritische Kommunikation vorgesehen. Eine Vielzahl von Service-Level-Agreements lassen sich jedoch vertraglich bei den Carriern von kritischen Infrastrukturen (und deren Services) definieren und/ oder durch leistungsfähige Mobilfunk-Anwendungen ergänzen. Die Handlungsfähigkeit der Sicherheitsbehörden beim absoluten Notfall zu gewährleisten, bleibt ein hohes Gut staatlichen Handelns und erfordert Redundanzen für die einsatzkritische Kommunikation.

Betreiber von kommerziellen Mobilfunknetzen bzw. Sprach- und Datenkommunikationsnetzen richten die Eigenschaften dieser Netze streng an den Bedürfnissen und Anforderungen der jeweiligen Nutzer aus. Somit bestehen Einschränkungen bei der geografischen Netzabdeckung, der Leistungsfähigkeit (im Allgemeinen erfolgt eine Überbelegung der Netzkapazität im Verhältnis zu den Nutzern) und der Zuverlässigkeit bzw. Verfügbarkeit in Sondersituationen, wie Stromausfall oder Naturereignisse. Teilweise lassen sich diese Einschränkungen durch organisatorische oder technische Maßnahmen kompensieren, oft aber nicht in dem für die Erfordernisse kritischer Kommunikation notwendigen Umfang.

Teile der Funktionalität im heutigen BOS-Netz lassen sich mit den Möglichkeiten kommerzieller Netze im Sinne einer Schnittmenge abbilden, allerdings nicht in jedem Fall mit der benötigten Qualität (z. B. Priorisierung). Die verfügbaren Bandbreiten liegen insbesondere in Ballungsräumen meist weit über denen im BOS-Netz, in einigen geografischen Gebieten hingegen sind diese unterdurchschnittlich.

Deshalb lässt sich die derzeitige Situation der kommerziellen Netze wie folgt zusammenfassen:

- Hohe Sicherheit
- Hohe Verfügbarkeit, keine Redundanz
- Hoher Datenschutz
- Hohe Funkabdeckung in Ballungszentren und Bereichen großen öffentlichen Interesses
- Volle Kompatibilität
- Hohe Dienstqualität
- keine PMR-spezifischen Leistungsmerkmale wie Einzelruf, Gruppenruf, Rufpriorisierung, SDS etc. verfügbar
- Hohe Service-Erwartung

4.2. Synergieanforderungen

Wird in Zukunft ein kombiniertes Netz betrieben, bei dem Sprachdaten über ein behördliches Funknetz (z. B. TETRA, missionskritisch) und sonstige Daten über ein kommerzielles Funknetz (IP-fähig, breitbandig) transportiert werden, müssen diese Sicherheitsanforderungen auf beide Netze (behördliches BOS Sprachfunknetz und BOS Datenfunknetz) übertragen werden. Dies gilt insbesondere für die Vertraulichkeit von Informationen, unabhängig davon, ob diese als Sprache oder in Form von Daten übermittelt werden.

Der Einsatz von kommerziellen Funknetzen für die Datenkommunikation im BOS Digitalfunk würde es erforderlich machen, dass sämtliche Nutzdaten im Netz des kommerziellen Anbieters durchgängig und VS-konform verschlüsselt werden. Dies betrifft einerseits die Daten, die über die Luftschnittstelle kommuniziert werden, aber auch Daten, die über das Netz des Providers über eigene Netze bis zum BOS Kernnetz transportiert werden. Die Mitarbeiter des Providers dürften keinen Zugriff auf diese sensiblen Daten haben.

Schwieriger gestaltet sich dies jedoch bei der Verschlüsselung von Funknetz-spezifischen Systemdaten (Authentisierungsdaten, Steuerungsdaten, Berechtigungsdaten, Protokolldaten, Konfigurationsdaten, Verkehrsdaten, etc.). Diese Daten können zwar von Standort zu Standort, aber nicht durchgängig verschlüsselt werden, da der Provider diese Daten in den Betriebsstandorten des Providers benötigt, um seine Dienste überhaupt zu erbringen und aufrechtzuerhalten. Ein Mitarbeiter eines kommerziellen Funknetzproviders hat damit die Möglichkeit, diese Daten einzusehen. Dabei entsteht jedoch auch die Gefahr des Missbrauchs dieser nicht zu verschlüsselnden Metadaten. Der Mitarbeiter könnte z. B. den Standort (die Funkzelle) eines bzw. sogar aller BOS-Endgeräte und damit auch aller Einsatzkräfte feststellen. Ein Mitarbeiter kann auch ermitteln, welches Gerät wann eine Verbindung zu einem anderen Gerät aufgenommen hat. Ein Mitarbeiter kann ein Endgerät auch für den Netzbetrieb freischalten oder sperren.

Letztendlich könnten die Authentisierungsdaten, Steuerungsdaten, Berechtigungsdaten, Protokolldaten, Konfigurationsdaten, Verkehrsdaten etc. im eigenen WAN des Funknetzproviders auch von Dritten abgehört und für weitere Angriffe missbraucht werden, da deutsche Funknetz-Provider in ihren eigenen Netzen derzeit keine VS-konforme Verschlüsselungstechnik verwenden.

Von jedem kommerziellen Anbieter eines solchen BOS Datenfunknetzes müsste daher ein hochsicherer VS-konformer Datenfunknetzbetrieb für die BOS-Organisationen gefordert werden, der entsprechend gesichert und von sonstigen **Netzen des Providers personell, organisatorisch und physikalisch/logisch getrennt und zertifiziert** ist.

5 Organisations- und Betriebsoptionen BOS in Deutschland

5 Organisations- und Betriebsoptionen – Digitalfunk BOS in Deutschland

Aus den dargestellten Synergiechancen ergeben sich Vorteile aber auch Defizite. Deshalb sollen nachfolgend auch diese beleuchtet werden und auch aus Sicht des heutigen BOS Digitalfunknetzes in Deutschland Empfehlungen bzgl. der betrieblichen, technischen und organisatorischen Gesichtspunkte gegeben werden.

5.1. BOS Digitalfunknetz in Deutschland Vorteile und Defizite

Deutschland hat mit dem dedizierten Digitalfunknetz großes Potential, die Aufgaben und Herausforderungen der Sicherheitsbehörden zu bewerkstelligen. Dies gelingt überwiegend gut, hat aber Verbesserungsmöglichkeiten.

Insbesondere ist die Aufteilung der Verantwortlichkeiten zwischen zentralem Betrieb und Systemlieferant (Wirknetz) verantwortlich für einen hohen Abstimmungsbedarf.

Es lassen sich folgende Vor- und Nachteile stichwortartig benennen:

5.1.a. Vorteile:

- Kein Zusammenbruch der Kommunikation bei Höchstanforderung
- Kein unbefugtes Abhören
- SDS, Status, Alarmierung läuft im Hintergrund über Organisationskanal
- Keine Überreichweiten
- Einzelruf- und Telefonie-Möglichkeit erhöht Gruppen-Gesprächs-Verfügbarkeit
- Bündeleffekt erhöht parallele Kommunikationsmöglichkeit

5.1.b. Defizite:

- Leitstellenzuordnung für Status-, GPS- und Notruf-Funktion führt zu Scanbetrieb
- ressourcenintensive Nutzung der Kurzdatenübertragung
- Keine Nutzung der Paket-Datenübertragung
- Begrenzte Anzahl der möglichen Gruppenadressen

- Keine flächendeckende Funkversorgung für Handfunkgeräte
- Unzureichende Funkausleuchtung der Inhouse-Bereiche führt zu Wildwuchs bei Objektfunkanlagen
- keine ausreichende Berücksichtigung der BOS-Belange und Endanwenderbedürfnisse

5.2. Empfehlungen

Es ergeben sich wegen der oben dargestellten Vorteile und Defizite folgende **Empfehlungen**:

- zentral geplantes, errichtetes und betriebenes Funknetz (Generalunternehmer), dadurch einheitliches Accessnetz und einheitlicher Standard bei Ausstattung der Standorte
- Schaffung einer schlanken und effektiven Organisation zum **Anforderungsmanagement** aus Länder, Bund und Generalunternehmer.
- enge Abstimmung bei der Planung und während des Betriebes zwischen Generalunternehmer und BOS-Vertretern (Anforderungsmanagement) zur Berücksichtigung einsatztaktischer Anforderungen an die Systemtechnologie und Erarbeitung von diesbezüglichen Lösungen.
- Berücksichtigung von zukünftigen Innovationszyklen der Systemtechnik und absehbaren Anforderungen in Bezug auf Funktionalität und Kapazität während der Planungsphase.
- auch Planungen (Funk- und Festnetz) im Rahmen des Change Managements (während des Betriebes) sollten vom Generalunternehmer (und nicht von anderer Stelle) durchgeführt werden (klare Verantwortungszuordnung).
- möglichst Berücksichtigung von Systeminfrastrukturen mehrerer Hersteller (falls technisch realisierbar → Schnittstellen und Verantwortlichkeiten) zur Reduzierung der Hersteller-Abhängigkeit
- Beibehaltung der betrieblichen Struktur mit autorisierten Stellen/vorhaltenden Stellen der Länder und technischem Betrieb.
- Nutzung von standardisierten Diensten und Leistungsmerkmalen (möglichst wenig »Sonder«-BOS-Anforderungen), dadurch werden Kosten gesenkt und gleichzeitig die Kompatibilität zwischen Endgeräten und Systeminfrastruktur erhöht.

- ausreichende Berücksichtigung von länderspezifischen Anforderungen und Lösungen sowie die Möglichkeit von eigenverantwortlichem Einsatz und Betrieb dieser (z. B. Ausstattung und Einsatz von spezifischer Systemtechnologie, wie mobilen Basisstationen).

- eine Schärfung der Rollen nach **Digital Service Provider und Digital Service Enabler**.

5.3. Problemstellung für Organisations- und Betriebsmodelle in Deutschland

Denkbar sind die unterschiedlichsten Formen von Organisations- und Betreibermodellen (Eigenbetrieb, Outtasking, Outsourcing, Fremdbetrieb unter Beachtung hoheitlicher Interessen). Diese haben unterschiedliche Stärken und Schwächen. Abstimmungen innerhalb des behördlichen Ökosystems sind schwer umzusetzen. Eine zukünftige Herangehensweise muss zusätzlich Benutzer und Anwender sowie Hersteller und Integratoren einbinden und deutlich agiler zu Lösungen kommen. Hinzukommen muss zudem eine bessere Einbindung der Nutzergruppen also der Endanwender im täglichen Dienst.

Für die einheitliche Umsetzung ist entscheidend, wie schnell und flexibel die Anforderungen von den Endnutzern mit den technischen Möglichkeiten und den zentralen Vorgaben (z. B. Standards, Sicherheit abgeglichen und Nutzer) in den Betriebsablauf eingebunden werden können.

Eines der Haupthandlungsfelder ist die agile Ertüchtigung der Betriebsabläufe mit dem Ziel schnellerer Umsetzung aktueller betrieblicher Anforderungen und neuer technologischer Entwicklungen. Die Steuerungsverantwortung sollte an zentraler Stelle liegen und die Anforderungen von Bund und Ländern im Rahmen von Gremien einbinden.

Bisher konnte oft nur zu langsam auf betriebliche Anforderungen reagiert werden. Die Einrichtung eines Architektur- und Technologiegremiums inkl. dessen Einbettung in Entscheidungs- und Beschaffungsprozesse ist notwendig, ohne jedoch zusätzliche Verzögerungen in den Abläufen zu implizieren.

Das erfordert klar definierte Prozesse inkl. der zugehörigen Rollenbeschreibungen, die regelmäßig an aktuelle Entwicklungen angepasst werden müssen. Um in schneller Folge Prozessdefinition, -planung und -implementierung zu durchlaufen, müssen geeignete Werkzeuge zum Einsatz kommen, mit deren Hilfe sich aus den standardkonformen Prozess- und Rollenbeschreibungen heraus Arbeitsanweisungen bis hin zu unterstützenden Anwendungen generieren lassen.

Sofern beim Betrieb mehrere Partner zur Erbringung von Einzelaufgaben beteiligt sind, sind diese klar zu definieren, sauber gegeneinander abzugrenzen und die Erbringung der Serviceaufgaben durch ein Servicemanagement auf Auftraggeber Seite zu verifizieren. Hier sollte auch das Qualitätsmanagement angesiedelt sein, um jederzeit den Grad der Gesamtservicequalität benennen zu können und kritische Bereiche zu identifizieren.

5.4. Herausforderung Personal und Fachkräfte

Für eine seriöse Personalaufwandsabschätzung sind die Anforderungen an den Betreiber entscheidend, auch das gewählte Organisationsmodell hat hierauf Einfluss.

Beim Eigenbetrieb muss ein ausreichender Personalpool für alle denkbaren Lagekonstellationen vorgehalten werden. Werden Betriebsleistungen nicht aus der eigenen Organisation bzw. mit eigenem Personal erbracht, muss die Erfüllung der vorgegebenen betrieblichen Anforderungen in Servicevereinbarungen vertraglich abgesichert werden. Damit liegt die Verantwortung für die Personalvorhaltung beim gewählten Vertragspartner. Die Planung sollte in erster Linie die geforderten SLA, die Anforderungen bezüglich Verfügbarkeit, Sicherheit und Vertraulichkeit und damit auch die erforderlichen Reaktionszeiten berücksichtigen. Für die Netzplanung und Serviceleistungen ist nach dem Abschluss der Aufbauphase eines neuen bzw. auch überarbeiteten Datenfunknetzes ein geringerer Personaleinsatz absehbar, sofern zwischenzeitlich keine Veränderungen der ursprünglichen Anforderungen definiert werden.

Weiterhin sind bei der Aufwandsabschätzung für Personal die verteilten Zuständigkeiten zwischen zentraler Betriebsführung und ggf. dezentral erbrachten Leistungspaketen zu berücksichtigen. Auch in diesem Bereich muss eine flexible Personal- und Einsatzplanung gestützt auf das aktuelle Anforderungsprofil erfolgen.

Eine optimierte Personalplanung wird unmittelbar aus den Rollenbeschreibungen und aus den definierten Prozessen und Aufgaben abgeleitet. Diese können unmittelbar mit Personalplanungswerkzeugen verknüpft werden, sodass eine flexible und schnelle Anpassung vorhandener personeller Ressourcen an veränderte Prozesse und Aufgabenstellungen möglich wird und Engpässe vermieden werden können, da bereits zum Zeitpunkt von Aufgaben- bzw. Prozessänderungen die Auswirkungen auf den Personalplan deutlich werden. Damit wird ein zusätzlicher zeitlicher Spielraum für die Personalbeschaffung erschlossen.

6 Internationaler Vergleich

6 Internationaler Vergleich

Wenn man sich mit einem großen Projekt bundesweit beschäftigt, ist die Frage zu stellen, wie es andere Staaten machen.

Die Telekommunikationswelt befindet sich seit einiger Zeit im Umbruch. Dieser Wandel zieht signifikante Veränderungen bei den potenziellen Kommunikationsanbietern und ebenso bei den Herstellern von entsprechenden Komponenten und Geräten nach sich.

Andere Länder verfolgen die Zweigleisigkeit von Sprechfunk mit TETRA und Datenübertragung mit LTE. Im Ausland wird z. B. bereits die Nutzung verlegefähiger oder mobiler LTE-Netze, speziell in militärischen Operationen genutzt. Eine LTE-Basisstation für den Fahrzeugeinbau hat in etwa das Volumen eines Schuhkartons und eine Leistungsaufnahme von ca. 60 Watt. Eine solche Station ermöglicht die Versorgung von ca. 100 Teilnehmern in einem Radius von 5-8 km. Eine Erweiterung auf ein komplettes LTE-Netz inkl. Management ist kommerziell verfügbar.

Im Rahmen der Digital Government Strategy der US-Behörden wurde beispielsweise eine »Mobile Security Reference Architecture« (MSRA) erarbeitet. Das Dokument zur Federal MSRA konzentriert sich auf die sichere Verwendung von mobilen Endgeräten und Infrastrukturen, die für die Nutzung von IT-Ressourcen der US Bundesbehörden eingesetzt werden. Die MSRA bietet einen Überblick über die erforderlichen Architekturkomponenten im Zusammenhang mit dem Einsatz von mobilen Endgeräten und Infrastrukturen sowie Beispiellösungen zur Minderung der Sicherheitsrisiken. Wie oben beschrieben, wurde aus dieser Referenzarchitektur bereits eine Ausprägung für deutsche Behörden abgeleitet, die an die vom BSI definierten Rahmenbedingungen angelehnt ist.

7 Anforderungskatalog für künftigen Digitalfunk der BOS

7 Anforderungskatalog für künftigen Digitalfunk der BOS

Wird angenommen, dass in Zukunft ein kombiniertes Netz verwendet wird, in dem Daten über ein kommerzielles Funkdatennetz (IP-fähig, breitbandig) transportiert werden, müssen diese Sicherheitsanforderungen auch im Netzbetrieb des kommerziellen Mobilfunkfunknetzbetreibers erfüllt werden. Dazu unter Berücksichtigung der Anforderungen aus der Sicht der Unternehmensexperten im Einzelnen:

7.1. Sicherheit (physische und Datensicherheit)

- Erfüllung der Anforderungen aus dem BSI-Grundschutzhandbuch
- Alarmsicherung der Standorte (ggf. mit Video-Überwachung)
- Verschlüsselung der zu übertragenden Daten in einem zu definierenden Umfang (Ende-zu-Ende-Verschlüsselung oder Verschlüsselung von Teilstrecken etc.)
- Ausreichende Standortsicherheit und (Geo-)Redundanz des Network Operation Centers des Netzbetreibers
- Möglichkeit der Deaktivierung von Endgeräten
- Möglichkeit der Ortung von Endgeräten

7.2. Verfügbarkeit (z. B. Mindestlaufzeit nach Stromausfall)

- vollständig redundante (knoten- und kantendisjunkte) Infrastruktur (insbesondere Access und Core Network)
- »Netzhärtung«: Sicherstellung einer Grundversorgung für Sprachkommunikation (Fahrzeugfunkversorgung) mit einer netzunabhängigen Stromversorgung über einen Zeitraum von mindestens 72 Stunden. Dieses ist auch durch das anbindende Access und Core Network sicherzustellen (Stichwort: Netzersatzanlagen)
- Einsatz von mobilen Systemen zur temporären Netzerweiterung und zum autarken Netzbetrieb (mehrzellig)

7.3. Funkabdeckung (Geographisch, Bevölkerung, Gebäude-durchdringung)

- Dieses ist länderabhängig. In Ländern, in welchen BOS-Kräfte digital (also mit TETRA) über Pager alarmiert werden, ist eine flächendeckende Funkversorgung bis in die Gebäude hinein (Berücksichtigung der Gürteltrageweise) erforderlich, da die Einsatzkräfte sonst z. B. nicht in ihren Wohnungen oder am Arbeitsplatz erreichbar sind.[1]
- Das System muss eine Funkabdeckung der Einsatzkräfte für Handheld Radio Terminals (HRT) in Gürteltrageweise sicherstellen. Wie diese technisch wirtschaftlich hergestellt wird (z. B. über Fahrzeug-Repeater und Kleinzellen im ländlichen Raum oder andere technische Konzepte), ist zu diskutieren.
- Insbesondere für BOS ist eine technische Möglichkeit vorzusehen, eine In-House-Versorgung herzustellen (sog. BOS-Objektversorgung). Diese muss beim Netzdesign bereits mit berücksichtigt werden, da hierfür ggf. auch im Access und Core Network Kapazitäten zur Verfügung gestellt werden müssen.
- Bei der Funkplanung sollte ebenfalls die Bedürfnisse von Spezialeinheiten berücksichtigt werden (besondere Applikationen, Laufzeitanforderungen, verdeckte Trageweise von Endgeräten, getarnte Antenneninstallation an Fahrzeugen etc.).
- Funkabdeckung für Luftfahrzeuge bis in Höhen von 5.000m (Hubschrauber- und Drohnenanbindung).
- Bei Funknetzen für BOS ist ein auf Erlang B/C bzw. alleinig auf Bevölkerungsdichte basierender Ansatz zur Kapazitätsberechnung nicht zielführend, da im Einsatz-/Katastrophenfall z. T. erhebliche Netzressourcen auch dort zur Verfügung stehen müssen, wo öffentliche Mobilfunknetze keine oder wenige Ressourcen zur Verfügung stellen. Die Dimensionierung des Funknetzes für die BOS muss daher basierend auf Einsatz- und Gefahrenschwerpunkten erfolgen. Dabei müssen auch Strategien zum schnellen Einsatz von mobilen Basisstationen bzw. ad hoc aufgesetzten autarken Netzen erarbeitet werden, um größtmögliche Flexibilität bzw. Verfügbarkeit des Funknetzes zu erzielen.

1 Nicht nur Länder mit Alarmierung über TETRA (BY, HE) haben höhere GAN-Stufen. HH hat und BE bekommt eine dichte Versorgung, andere haben nur taktisch relevante Gebiete höher versorgt. In den Wohnungen stehen derzeit die Ladegeräte mit Antennenanschluss und Außenantenne, um die Erreichbarkeit auch in Gebäuden zu ermöglichen. Dies macht jedoch auch abhängig von diesen Stationen und sollte in Zukunft auch ohne zusätzliche Hardware sichergestellt sein.

7.4. Technikkompatibilität und Frequenzen

- Die Komponenten der Netzinfrastruktur sollten möglichst standardisiert sein, um nicht von einem Hersteller/Lieferanten abhängig zu sein. Dabei sollten sinnvolle Schnittstellen hierfür definiert werden, die ein klare Verantwortungstrennung ermöglichen und einen Weiterbetrieb des Netzes bei Herstellerwechsel ermöglichen.
- durch eine standardisierte Luftschnittstelle sollte ein möglichst breites Herstellerspektrum für die Endgeräte genutzt werden können.
- Bestehende BOS-Infrastrukturen und Anwendungen müssen an das Funknetz angeschaltet werden können, hierfür müssen ebenfalls möglichst standardisierte Schnittstellen zur Verfügung stehen.
- Für die BOS müssen dedizierte/exklusive Frequenzen im ausreichenden Umfang zur Verfügung stehen.

7.5. Grenzüberschreitender Einsatz

- Eine »Nacheile« in grenznahe Gebiete muss sichergestellt sein. Hierzu muss das Netz noch einen gewissen grenznahen Bereich (z. B. 10 km) des Nachbarlandes abdecken
- für internationale Einsätze von BOS-Kräften muss eine technische Möglichkeit geschaffen werden, wie diese mit ihren eigenen Endgeräten im fremden Netz bzw. mit Heimat-Kräften und Heimat-Leitstellen kommunizieren können

7.6. Endgeräte,

- robuste Handfunkgeräte (HRT),
  - robust für den Einsatz mit Handschuhen geeignet
  - mit dedizierten Schnittstellen zur Anschaltung von Zubehör (z. B. Handmikrofon)
  - ausreichend Speicherplatz für die Beweissicherung und Speicherung von Einsatzdaten
- Endgeräte für verdeckte Trageweise (Personenschutz, Observation etc.) inkl. notwendigen Zubehörs
- Fahrzeugfunkgeräte (Mobile Radio Terminals, MRT) mit flexiblen Ein- und Ausgabe-Medien (Tablet)
- ggf. Pager zur Alarmierung von Einsatzkräften

2 Ergänzung: Zusammenhängende Fr-Pakete. Hersteller haben zu den bisherigen, verstreuten BOS- Fr-Paketen schon Bedenken wegen der Realisierungsmöglichkeit geäußert.

- Zubehör zum Einbau der Endgeräte in Fahrzeugen, insbesondere auch in Spezialfahrzeugen von Feuerwehr und Polizei, Rettungsdienste und Katastrophenschutz (bis hin zu Hubschraubern und Booten)
- Fixed Radio Terminals (FRT) für BOS Dienststellen
- Systeme zur de- und zentralisierten Programmierung von Endgeräten (z.B. über LAN/WAN und IP-Schnittstellen an den Ladehalterungen der Endgeräte bzw. idealerweise sicher over the air
- Die BOS-Anwender sind es gewohnt unter mehreren Anbietern wählen zu können > volle Kompatibilität.
- gewohnte Nutzung von Diensten, Apps wie aus den Mobilfunknetzen mit privaten Geräten

7.7. Dienste

- Einzelruf (semiduplex, vollduplex)
- Gruppenruf
- Notruf zu frei definierbaren Zielen (auch Gruppen)
- gleichzeitiges Mithören von mehreren Gruppen
- dynamische Gruppenbildung
- Rufprioritäten (verdrängend, nicht verdrängend)
- Short Message/Data Service (im TETRA: SDS)
- Übertragung von Statusmeldungen (z. B. Einsatzstatus)
- Ortung von Endgeräten über GPS/Galileo und automatisierter SOS Ruf
- Übertragung von Fotos bzw. Videos (z. B. Helmkamera, Body Cam)
- Ambience Listening (Abhören der Umgebung eines Endgerätes z. B. durch die Leitstelle)
- Schnelle (adhoc) gruppenbezogene Zuweisung von Ressourcen (zur Laststeuerung im Netz)
- Direktmodus (im TETRA: Direct Mode Operation, DMO): Kommunikationsmöglichkeit von Endgerät zu Endgerät ohne Nutzung der Netzinfrastruktur

7.8. Dienstqualität (insb. erforderliche Bitraten und Latenzzeiten)

- Kurze gesicherte Rufaufbauzeiten, insbesondere beim Gruppenruf (ca. 500 ms)
- Bitraten entsprechend den erforderlichen Dienste (siehe oben)
- Hohe gesicherte Sprachqualität. Jede Silbe von Einsatzbefehlen (auch bei einem Handover im Netz) muss die Einsatzkräfte sicher erreichen
- Dokumentation erfolgt idealer Weise bei den Anwender-Systemen

7.9. Operativer Zugriff der Behörden auf Netzressourcen im Katastrophenfall

- Ein operativer Zugriff muss sofort und exklusiv sichergestellt werden (nicht nur im Katastrophenfall)
- Verfügbarkeit im Black-Out und Stromausfall muss berücksichtigt werden. Da die Mobilfunknetze sofort zusammen brechen, müssen diese ebenfalls als Teil der Katastrophenhilfe ertüchtigt werden
- Einfacher Service für die Infrastruktur
- Hohe Netzressourcen ggf. auch mit vorgehaltenen mobilen Einsatzsystemen im Katastrohen-Fall für Behörden Sprechfunk / Daten Priorität können unterschiedlich eingestuft sein

8 Zusammenfassung

Zusammenfassung

Die Weiterentwicklung des Digitalfunks für BOS ist dringend erforderlich und eine wesentliche Aufgabe der Sicherstellung der Leistungsfähigkeit von BOS. Die zukünftigen Herausforderungen des Einsatzes und der effizienten Einsatzplanung machen eine zuverlässige und integre Kommunikation zwischen den Einsatzkräften, der Leitstellen und anderen Beteiligten unabdingbar. Dabei wird es zunehmend auch auf die Ausnutzung breitbandiger Kommunikationsmöglichkeiten ankommen, um auch Einsatzdaten zu kommunizieren und auswertbar zu machen. Nicht zuletzt militärische Anwendung von z. B. Videoübertragung und Sensordaten im Einsatz des Führungskommandos zeigen bereits, welche Dienste auch im Umfeld der inneren Sicherheit zukünftig nutzbar werden. Erste Projekte mit Bodycams bei Polizeien laufen bereits. Auch Katastrophen-, Rettungs- und Feuerwehreinsätze bieten zahlreiche Beispiele sinnvoller Breitbandkommunikation.

Die derzeitige Form des TETRA Standards ist nicht mehr zukunftssicher und es besteht dringender Handlungsbedarf, um den zukünftigen Anforderungen gerecht zu werden. Der aktuelle Standard muss in zügigen Prozessen unter Mitwirkung der Anwender reformiert werden, da er sonst nicht überlebensfähig ist. Die derzeitigen Prozesse in den Standardisierungs-Gremien (u.a. ETSI) sind dafür zu starr und langwierig, da in der jüngeren Vergangenheit auch zu wenig intensiv an einer Fortentwicklung gearbeitet wurde. Es muss eine Form der Koexistenz und Integration mit bestehenden Breitband-Kommunikationsstandards, insbesondere der verbreiteten LTE-Technologie, geschaffen werden, um vorhandene technische Möglichkeiten effizient ausschöpfen zu können.

Bitkom befürwortet deshalb für die Zukunft des Digitalfunks für BOS (DF BOS) die Verfolgung einer kombinierten Strategie. Diese sollte sowohl den TETRA als auch den LTE Standard für den DF BOS nutzbar machen. So ist eine Möglichkeit gegeben, während der Weiterentwicklung von TETRA sowohl die Vorteile einer krisensicheren Sprachfunkübertragung als auch der digitalen Breitbandkommunikation zu nutzen. Zwingend hierfür erforderlich sind die nahtlose Integration der genannten Standards und die Sicherheit des Breitbandkanals über LTE.

Dabei ist insbesondere auf eine frühzeitige Einbindung der Beteiligten zu achten. Die Hersteller, Betreiber und vor allem die Endnutzer müssen in die Definition der Anforderungen und die Planung eingebunden werden. Bereits heute nutzen viele Einsatzkräfte in Situationen, in denen der Funktionsumfang des TETRA-Endgerätes nicht ausreicht ihr privates Smartphone, um beispielsweise Karten und Lageinformationen abzurufen oder wegen der einfacheren Bedienbarkeit Direktrufe herzustellen. Insofern sollten die zukünftigen Endgeräte ebenfalls Wert auf die Nutzerfreundlichkeit und die Usability legen und sich an den Bedienkonzepten aktueller Mobilgeräte orientieren.

Auch die internationale Zusammenarbeit auf diesem Gebiet muss gestärkt und in der Umsetzung auch organisatorisch berücksichtigt werden. Digitalfunk ist auch grenzüberschreitend ein Zukunftsthema.

Alles in allem bedarf es einer schnellen, pragmatischen Lösung zur Reduzierung der Defizite bei der Abdeckung bestehender Anforderungen an die Digitalfunk-Infrastruktur. Eine solche Lösung sollte mit den verfügbaren Ressourcen erbracht werden können, bestehende Funktionen für die Anwender sinnvoll ergänzen und nutzerzentriert gestaltet werden.

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon gut 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom