

## Positionspapier über die Notwendigkeit ausfallsicherer Breitbandanbindungen im Bereich der Feuerwehr

Die praktischen Tätigkeiten bei der Gefahrenabwehr erfordern zur Führung und Lage sowie zur Aufklärung und Koordination in Einsatzlagen immer mehr digitale Verfahren zur Zielerreichung.

Hier kommen nicht nur lokale Anwendungen mit direkten Vernetzungen in Betracht, auch Anbindungen über lange Strecken sind hierbei erforderlich. Zunehmend größere Datentransportkapazitäten sind zu berücksichtigen, die derzeit im Regelfall nur über kommerzielle Provider bereitgestellt werden können.

### **Anwendungen und Sicherstellung der Verfügbarkeit bei Ausfall**

Anwendungsfälle sind hierbei im Regelbetrieb eingeführte Verfahren, aber auch ereignisabhängige Verfahren wie unter anderem:

- a. Im Einsatzfall die Ebenen übergreifende Anbindung von Führungseinrichtungen der Gefahrenabwehr (Stichwort Informationsraum mit gemeinsamen Lagebildern zu Lagezentren der Gefahrenabwehr und mitwirkenden Einrichtungen wie zum Beispiel Kliniken, Einsatzleitungen, Abschnittsleitungen);
- b. Redundante standortübergreifende Alarmierungswege unter Beachtung größerer Entfernungen und Zusatzalarmierungen mit Details zur Einsatzstelle und Details via Alarmausdruck;
- c. Digitaler Datenaustausch für medizinische Daten zwischen taktischen Einheiten im Rettungsdienst, Leitstellen, Kliniken und gegebenenfalls weiteren Einrichtungen im Gesundheitssystem. Datenübertragungen für Telenotarzt, IVENA und Dokumentationspflichten.
- d. Digitaler Datenaustausch mit einsatzunterstützenden Informationen zu taktischen Einheiten im Brandschutz und der Hilfeleistung (und Routingdaten, Objektinformationen, Einsatzinformationen...).
- e. Digitaler Datenaustausch zu Einrichtungen im Katastrophenschutz (Anbindung zur Bevölkerungsinformation, Notfallmeldestellen, Medien, Verwaltung)

Im Zuge der genannten Anwendungen haben sich bereits Verfahren im Regelbetrieb zur Nutzung gefestigt. Diese Verfahren basieren in der Regel auf einer vertraglichen Nutzung von Kommunikationswegen kommerzieller Betreiber im Sinne der Übertragungswege (Mobilfunknetze), aber auch in der Bereitstellung der Serverkomponenten (zum Beispiel Hosting Server durch Dienstleister außerhalb eines möglichen Zugriffsbereiches innerhalb behördeneigener Infrastruktur).

Zur Gewährleistung der Verfügbarkeit der Dienste in der Gefahrenabwehr beim Ausfall der örtlichen Infrastruktur (zum Beispiel in Folge Stromausfall, Naturkatastrophen) gilt es, die in diesen Szenarien notwendigen Anwendungsbereiche zu identifizieren und die Betriebsbereitschaft der Verfahren zu priorisieren. In der Folge sind für unverzichtbar notwendige Verfahren Konzepte für einen sicheren Betrieb zu erstellen. Dies gilt insbesondere auch für notwendige Anwendungen bei Großschadenslagen und Katastrophen.

Der Ebenen übergreifende Datenaustausch zwischen den Führungseinrichtungen, die Sicherstellung der Alarmierungswege und der digitale Datenaustausch zu Einrichtungen des Katastrophenschutzes erfahren im Rahmen der Priorisierung im Regelfall die höchste Priorität.

Die Aufrechterhaltung des Datenaustausches für medizinische Daten und des Datenaustausches mit einsatzunterstützenden Informationen besitzt ebenfalls eine hohe Priorität und muss standortspezifisch bewertet werden. Eine Kompensation/Redundanz solcher Datenverfahren über Sprachübermittlung (Sprechfunk bzw. Drahtkommunikation) führt in der Regel zu einer Erhöhung der Arbeitslast in den bei solchen Szenarien ohnehin schon hochbelasteten Führungseinrichtungen.

### **Übersicht der derzeit für Datendienste in der Gefahrenabwehr verfügbaren Anbieter/Systeme (ohne Anspruch auf Vollständigkeit)**

Die Mobilfunknetze stellen hohe Datendurchsatzraten im Regelbetrieb sicher. Betrieben werden diese durch kommerzielle Betreiber ohne direkte Einflussmöglichkeit der BOS bezüglich Netzhärtung und Ausfallsicherheit. Es existieren zugesicherte Vorrangschaltungen, die jedoch im Datenverkehr (noch) nicht verlässlich

verfügbar sind. Bereits bei einer Überlastung von Mobilfunkzellen (noch ohne Ausfall der Infrastruktur) kann bereits die Betriebssicherheit gefährdet sein. Für den Nutzer sind Optimierungen durch eine parallele Nutzung verschiedener Provider vorstellbar. Hierfür sind beim Nutzer hochwertige Geräte notwendig, die zwischen den Netzen ereignisinduziert umschalten.

Im Tetra-Funknetz BDBOS ist derzeit keine Breitbandanbindung verfügbar; es ist (im Regelfall) nur eine sprachbasierte Kommunikation darstellbar. Mittel- bis langfristig sollen Breitbandanbindungen für die Gefahrenabwehr verfügbar werden (Zielzeitraum ab 2030). Technische Leistungs- und Sicherheitsniveaus sind noch nicht beschrieben.

Die Satellitenkommunikation (zum Beispiel über Iridium / BGAN / Inmarsat-Satelliten) bietet in Bezug auf die Datenanbindung oder Stromversorgung eine Ausfallsicherheit gegenüber Netzen mit gefährdeten Mobilfunkstandorten. Hierüber sind Daten und Sprachdienste nutzbar. Weitere Satellitennetze für Datendienste befinden sich im Aufbau und sind bereits (teilweise) verfügbar (zum Beispiel Starlink). Die Verfügbarkeit ist vom tatsächlichen Kommunikationsbedarf abhängig; bei der Auswahl des Anbieters ist dies zwingend zu beachten. Bei hohem Kommunikationsbedarf zeigen sich Einschränkungen an verfügbaren Kapazitäten, dies kann zum Abwurf von Teilnehmern in diesen Netzen führen. Eine verlässliche Priorisierung von BOS-Teilnehmern ist (bisher) nicht gegeben. Je nach Technologie ist eine mobile Anwendung dieser Verfahren nicht möglich. Es werden entweder feste Standorte benötigt oder entsprechende Services zur Festlegung und schnellen Anpassung der bodenbasierten Ausleuchtungsfläche sind beim Provider festzulegen.

Teilweise werden bereits eigene kommunale/Landes-/Bundesnetze als Drahtanschluss verwendet bzw. befinden sich im Aufbau (zum Beispiel Ausführung als passives Glasfaserkabel). Diese „eigenen“ Netze bieten für den Regelbetrieb eine sichere Datenkommunikation und im Regelfall ausreichende Bandbreiten. Die Ausfallsicherheit dieser drahtgebundenen Netze (zum Beispiel gegenüber Naturkatastrophen, mechanischen Störungen) muss dabei aber örtlich bzw. regional bewertet werden. Der mobile Einsatz ist in der Regel nicht möglich.

Richtfunkstrecken können als Redundanz oder Erweiterung kabelgebundener Systeme eingesetzt werden. Allerdings sind hier Sichtverbindungen erforderlich und die Standorte fest auszuwählen. Aufgrund hoher Auslastung ist die Verfügbarkeit und Genehmigung der nötigen Frequenzbänder fraglich.

Zu weiteren Rückfallebenen, zum Beispiel dem Ad-Hoc Netz (zum Beispiel WiMAX) finden derzeit Forschungen und Erprobungen statt. Zu berücksichtigen ist hier, dass „neue Netze“ im Ereignisfall erst aufgebaut werden müssen und daher nur eine begrenzte lokale Verwendung besteht. Auch die Anbindung an übliche Webdienste ist dabei fraglich.

### **Zusammenfassung und Bewertung**

Die Datenübertragung im Regelbetrieb ist etabliert. Eine ausfallsichere Datenübertragung für Ausfallszenarien (zum Beispiel Naturkatastrophen, Ausfall Infrastruktur) ist in der Regel zumindest für die Generierung von Lagebildern und zur Kommunikation zu Einrichtungen des Katastrophenschutzes notwendig.

Bundesweite zentrale und behördeneigene Lösungen werden präferiert. Diese sind derzeit jedoch noch nicht vorhanden. Entsprechende den Feuerwehren zur Verfügung stehende Breitbandfrequenzen sind zwingend erforderlich. Eine zeitnahe Bereitstellung über die BDBOS muss forciert werden.

Beim Aufbau der Netze muss ebenso an eine ausreichende In-House-Versorgung gedacht werden.

Auch eine Anbindung von Dienstleistern für die verwendeten, außer Haus betriebenen, Verfahren muss vorgesehen werden, um diese ebenso ohne Abhängigkeit von kommerziellen Netzwerkanbietern integrieren zu können.

Alternativ bleibt derzeit in der Regel nur die Verwendung kommerzieller Anbieter, die ihr Verfügbarkeitslevel jedoch nur eingeschränkt zusichern.

Zu beachten und vorzuplanen sind auch immer die (Hardware-)Schnittstellen des Datenaustausches und die verwendeten Softwareverfahren. Bei der Nutzung von Rückfallebenen muss die Ausfallsicherheit dieser Komponenten gegeben sein. Zudem sind die jeweiligen Netzwerkstrukturen und Anbindungsmöglichkeiten zu beachten.

Die Beachtung der IT-Sicherheit (zum Beispiel gegen Fremdzugriff) ist notwendig, die Verwendung von Online-Diensten oder Cloud Anbietern muss intensiv bewertet werden. Sofern diese entsprechend zertifiziert sind (zum Beispiel ISO/IEC-27000-Reihe) und mit hohen Sicherheitsstandards arbeiten, können diese verwendet werden. Eine Anbindung an die eigenen Netze über verschiedene Wege und mit Zutrittsrechten zu einem behördeneigenen Breitband-Netzwerk muss dabei geregelt geschaffen werden. Dies muss bei der Auswahl und beim Aufbau eines Netzes beachtet werden.

Bei der Auslegung der Systeme muss auch eine garantierte Netzkapazität für den vorgesehenen Benutzerkreis festgelegt und im Betrieb sichergestellt werden. Dabei sind nicht nur die Datenraten des Regelbetriebes, sondern auch die erhöhte Auslastung im Schadensfall zu berücksichtigen.

Berlin, 31. Juli 2023

Erstellt wurde dieses Positionspapier durch den Fachausschuss Leitstellen und Digitalisierung der deutschen Feuerwehren. Der Fachausschuss ist ein gemeinsames Gremium der Arbeitsgemeinschaft der Leiterinnen und Leiter der Berufsfeuerwehren in der Bundesrepublik Deutschland (AGBF bund) und des Deutschen Feuerwehrverbandes (DFV).

Ihr Kontakt: Carsten-Michael Pix / Telefon (030) 288 848 8-28 / E-Mail [pix@dfv.org](mailto:pix@dfv.org)

Haftungsausschluss: Das Positionspapier „Notwendigkeit ausfallsicherer Breitbandanbindungen im Bereich der Feuerwehr“ wurde nach bestem Wissen und unter größter Sorgfalt durch unsere Experten erstellt und durch die zuständigen Fachbereiche und das DFV-Präsidium geprüft. Eine Haftung der Autoren oder des Deutschen Feuerwehrverbandes ist jedoch grundsätzlich ausgeschlossen.