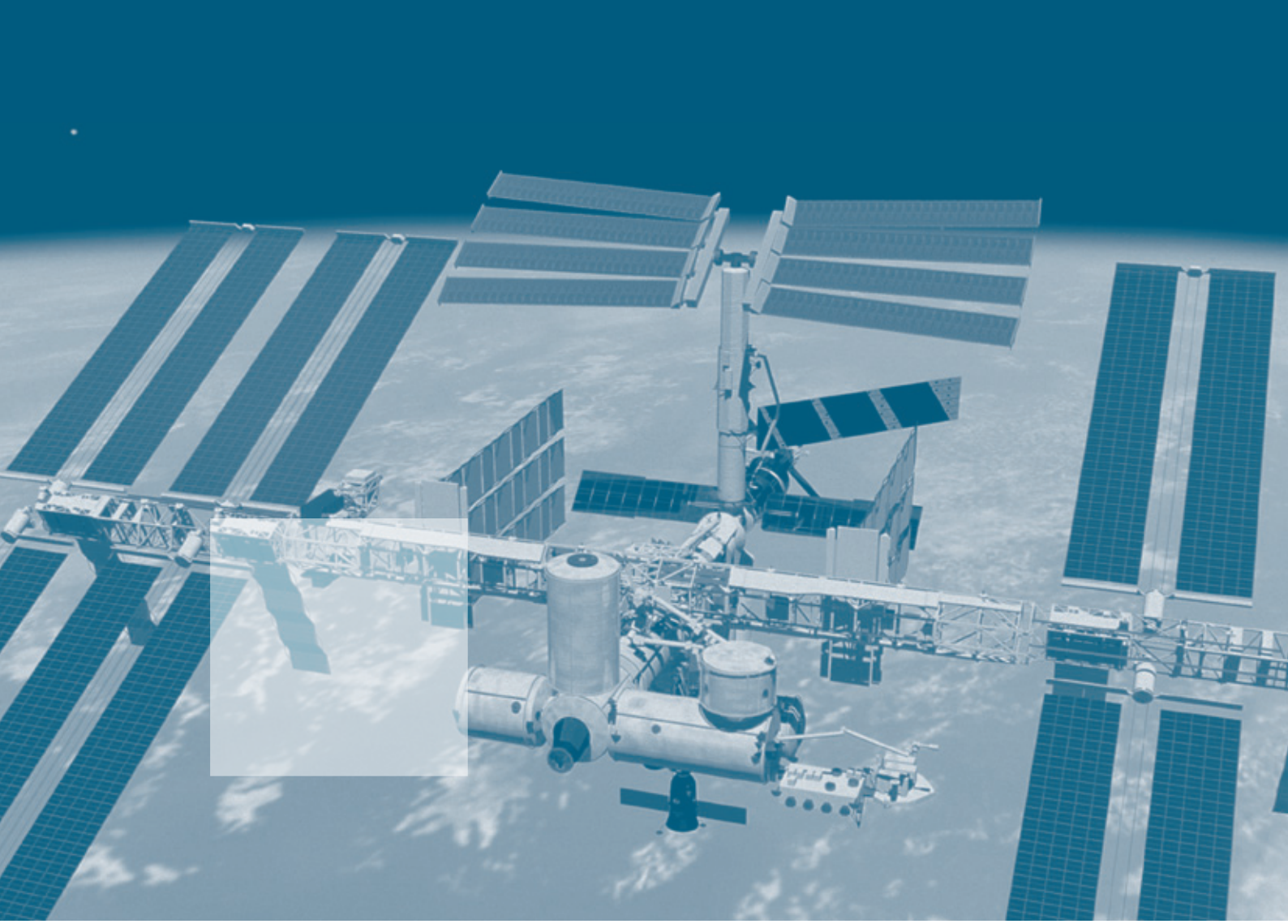

Krisenmanagement und Bevölkerungsschutz – Eine neue Qualität

Öffentliche Sicherheit aus Sicht der ITK-Industrie

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Marco Junk Tel.: 030.27576-133 m.junk@bitkom.org
Redaktion:	Marco Junk
Redaktionsassistenz:	Stefanie Brzoska
Gestaltung / Layout:	Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)

Krisenmanagement und Bevölkerungsschutz – Eine neue Qualität

Öffentliche Sicherheit aus Sicht der ITK-Industrie

BITKOM

Inhaltsverzeichnis

1 Vorwort

Albrecht Broemme,
Präsident der Bundesanstalt Technisches Hilfswerk (THW)

Deutschland verfügt über ein ausreichendes Potenzial an Hilfskräften und Material, um Schadenslagen abzuwehren. Insbesondere die 1,7 Millionen ehrenamtlichen Helfer bei Feuerwehren, Technischem Hilfswerk (THW), Deutsches Rote Kreuz (DRK), Arbeitersamariterbund (ASB), Malteser Hilfsdienst (MHD), Johanniter Unfallhilfe (JUH) und DLRG sowie Berufsfeuerwehren tragen dazu bei, dass die Bundesbürger auf eine gut ausgebaute und hoch verfügbare Schadensabwehr vertrauen können.

Damit bei schwierigen Schadenslagen, Großschäden oder Katastrophen die richtigen Entscheidungen getroffen werden können, ist die Verfügbarkeit von Informationen an den richtigen Stellen zur richtigen Zeit erforderlich. Diese Informationen müssen schnell weitergegeben und bedarfsgerecht bereitgestellt werden, denn verspätete Informationen sind genauso unbrauchbar wie eine nicht beherrschbare Informationsflut.

Interoperabilität und Vernetzung sind daher auch im Bevölkerungsschutz grundlegende Voraussetzungen. Um dies zu gewährleisten, müssen die technischen, rechtlichen und organisatorischen Konzepte für die verschiedenen Verwaltungsebenen und Handlungsbereiche entwickelt und realisiert sein.

Dies ist vor dem Hintergrund einer komplexen nationalen und internationalen Sicherheitsarchitektur eine anspruchsvolle Aufgabe. Unterschiedliche Akteure auf unterschiedlichen Ebenen bedingen eine komplexe Informationsstruktur, die sich dennoch durch eine überschaubare Bedienung auszeichnen soll.

Diese Herausforderungen der Gegenwart und der Zukunft an die Kompatibilität von Informations- und Kommunikationssystemen erfordern erhebliche Anstrengungen. Anstrengungen, die zweifellos die richtigen Investitionen sind, geht es doch um ein wertvolles Gut: unsere Sicherheit.

2 Bevölkerungsschutz: Eine neue Qualität

Bevölkerungsschutz, Krisen- und Katastrophenschutz oder doch besser Katastrophenmanagement? Die Bezeichnungen sind vielfältig, die Aufgaben jedoch eindeutig – Schadensfälle jeglicher Art und Dimension beherrschen, Menschenleben retten und in Notlagen helfen.

So eindeutig die Aufgaben sind, so vielfältig sind die unterschiedlichen Akteure. Auf der einen Seite stehen die klassischen Hilfsorganisationen wie das Technische Hilfswerk, die Bundeswehr, die Polizeien, die Feuerwehren und die Rettungsdienste wie das Rote Kreuz, die Johanniter oder der Arbeiter Samariterbund, um nur einige der Hilfs- und Wohlfahrtsorganisationen zu nennen, auf der anderen Seite die Innenministerien in Bund und Ländern, internationale Organisationen und nicht zu vergessen die Betroffenen wie Bürger, Industrien und Infrastrukturen.

Die Herausforderungen in einer vernetzten und globalisierten Gesellschaft sind komplex. Seuchen und Pandemien, Terroranschläge und der großflächige Ausfall von gesellschaftswichtigen Infrastrukturen erweitern die klassischen Großschadenslagen wie Unfälle durch technisches und menschliches Versagen.

Auch in Deutschland drohen immer größere Schadensereignisse, die infolge extremer Wettersituationen, dem Ausfall von lebenswichtiger Infrastruktur oder durch internationalen Terrorismus verursacht werden können. Bei großflächigen Gefahrenlagen nehmen Kommunikation und Interaktion zwischen allen Beteiligten in einem erheblichen Umfang zu.

Bis heute erfassen und verteilen viele Krisenstäbe die eingehenden Meldungen noch mit Vierfachvordrucken. Die Flut von Nachrichten kann jedoch mit diesen Instrumenten nicht mehr bewältigt werden, da mit dem Anstieg des Meldeaufkommens die Fehlerquote bei der Verarbeitung der Informationen exponentiell ansteigt.

Die Verantwortlichen der Gefahrenabwehr müssen daher neue Instrumente einsetzen, um das Informationsmanagement zu verbessern. Die Möglichkeiten der Informationstechnik und der elektronischen Vernetzung müssen genutzt werden, um den neuen Herausforderungen gewachsen zu sein.

Eine großflächige Gefahrenlage erfordert die Bündelung aller Kräfte. Durch die unterschiedlichen Zuständigkeiten und Fähigkeiten der einzelnen Akteure ist dies mit einem erheblichen Koordinierungsaufwand verbunden. Es ist daher dringend notwendig, ein übergreifendes Informations- und Kommunikationssystem zur Darstellung der Einsatzlage und zur Unterstützung der zentralen Koordination aufzubauen. Risiken müssen dokumentiert, Einsatzfälle trainiert und Methoden und Systeme installiert werden.

Die ITK-Industrie spielt hierbei eine wichtige unterstützende Rolle.

Die geplante Einführung des digitalen Behördenfunks (System TETRA) wird mittel- und langfristig im Bereich der Sprachkommunikation die Situation deutlich verbessern. Kurz- und mittelfristig muss sicherlich berücksichtigt werden, dass die deutschen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) jeweils eigene Zeitpläne für die Migration zum Digitalfunk erstellt haben. Vielerorts werden Feuerwehren noch lange ihre Trupps mit Analogfunk führen, während die Polizeien eher zügig den Digitalfunk einführen werden. Die Bundeswehr setzt das Digitalfunksystem TETRAPOL ein, welches nicht direkt zu TETRA kompatibel ist.

3 Forderungen

In der BITKOM Broschüre „Homeland Security – Vernetzte Sicherheit aus Sicht der deutschen ITK-Industrie“, Oktober 2005, wurde eine gesamtstaatliche Sicherheitsarchitektur grob beschrieben und ausgeführt, dass Informations- und Kommunikationstechnologien (ITK) bei der Lösung dieser Herausforderung eine entscheidende Rolle einnehmen.

3.1 Forderungen und Informationsstrategie

Die Informationsinfrastruktur für die Aufgabe Krisen- und Katastrophenmanagement sollte folgenden Elementen Rechnung tragen:

- Einsatzkräfte in Krisen- und Katastrophenfällen werden jeweils ereignisorientiert zusammengestellt
- Einsatzkräfte müssen in ständig wechselnden Gruppierungen mit Partnern zusammenarbeiten, personell aufwachsen und einheitlich agieren können.
- Einsatzkräfte müssen miteinander kommunizieren und Daten austauschen können, damit ein gemeinsames Lagebild entstehen kann und die abgestimmte Führung der Kräfte ermöglicht werden kann.
- Daher müssen die zu schaffenden Instrumentarien zum Informationsaustausch und zur Führung ein größtmögliches Maß an Flexibilität und Interoperabilität aufweisen.
- Die Autonomie und ggf. Autarkie der beteiligten Akteure darf durch das System nicht eingeschränkt werden.

3.2 Vorteile der Informationsarchitektur

Durch den Aufbau einer durchgängigen Informationsarchitektur entstehen für das Gesamtsystem Krisen- und Katastrophenmanagement eine Vielzahl von Vorteilen, z. B.

- Identifikation aller für die Bewältigung in Frage kommenden Organisationen mit ihren jeweiligen Fähigkeitsprofilen.
- Transparenz über organisationsübergreifende Prozesse und Schnittstellen.
- Identifikation von Optimierungspotenzialen in der organisationsübergreifenden Zusammenarbeit.
- Gesicherte Grundlage für die Weiterentwicklung und Standardisierung der IT-Unterstützung bei Planung und Durchführung von Hilfsmaßnahmen.

Gleichzeitig wird damit eine gemeinsame Planungsgrundlage für die beteiligten Organisationen und die anbietende Industrie geschaffen.

3.3 Handlungsnotwendigkeiten

Daher schlagen wir Umsetzungsmöglichkeiten mit folgenden Elementen einer gesamtstaatlichen Sicherheitsarchitektur vor:

Breitbandiges, leistungsfähiges und robustes Kommunikationssystem

Vorrangiges Ziel muss es sein, vorhandene und zukünftige Systeme interoperabel zu gestalten, stationäre und mobile Sensoren, Mitarbeiter sowie Führungs- und Einsatzzentren der beteiligten Sicherheits- und Hilfsinstitutionen einzubinden, um somit das virtuelle Gesamtsystem aufzubauen.

Kernforderung ist es, eine flexible IT-Infrastruktur zur Verfügung zu stellen, welche die Implementierung eines auszuwählenden Ansatzes ermöglicht und auch Änderungen bzw. Neuerungen während des Lebenszyklus unterstützt. Dabei ist die konsequente Nutzung von Standards durch alle Beteiligten sicherzustellen. Das Netz stellt damit die integrierte Plattform für die Aufgabenwahrnehmung dar.

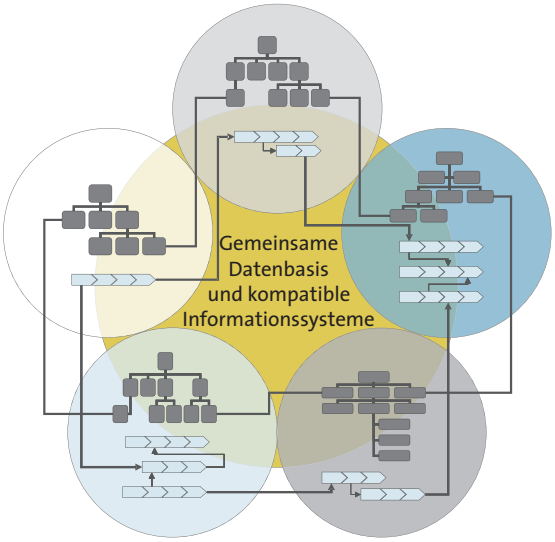

Abbildung 1: Gemeinsames Datenprozessmodell

Virtuelles Informations- und Leitsystem

Auf dieser flexiblen Basis-Infrastruktur kann die Architektur eines virtuellen Informations- und Leitsystems, das für alle Beteiligten nutzbar ist, aufbauen und folgenden Anforderungen genügen:

- Hohe Verfügbarkeit – zu jeder Zeit – an jedem Ort.
- Unterstützung sicherheitskritischer Organisationen.
- Möglichkeiten der Informationsverdichtung.
- Gemeinsamer Zugriff – rollengerecht: Personalisierter Zugriff auf die notwendigen Informationsdienste.
- Konsistente Daten – inhaltlich verlässlich: Basis für ein solches Datenmodell könnte das vom Bund (BBK) gemeinsam mit dem Land Hamburg entwickelte Datenmodell sein, welches in deNIS IIplus eine erste Implementierung erfahren hat.
- Mobile Informationsdarstellung: Die Darstellung muss den technischen Möglichkeiten und den Einsatznotwendigkeiten vor Ort automatisch angepasst werden.
- Integrierte Kommunikation: Sprache, Daten, Video, Fax und Funk im Lagezentrum ermöglichen auch unter Zeitdruck effiziente und fehlerarme Arbeit.

Aktionsplan für Interoperabilität von Prozessen, Organisation und Technik

Neben der technischen Interoperabilität darf die Abstimmung auf der Ebene von Prozessen und Organisationen (organisatorische Interoperabilität) nicht vergessen werden. Dieser Schritt erschließt die übergreifende Synergie zur Verbesserung des Katastrophenschutzsystems Deutschlands.

Standards bilden sich allerdings nicht von selbst, sondern müssen durch alle Beteiligten gemeinsam, strukturiert und gewollt erarbeitet werden. Der zu erarbeitende Interoperabilitätsplan muss dabei diese Dimensionen berücksichtigen.

Gastbeitrag: Bernhard Corr, Referatsleiter deNIS, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Wenn Schadenslagen Verwaltungsgrenzen und damit Zuständigkeiten von Behörden und Organisationen überschreiten, kommt es auf einen schnellen und sicheren Informationsaustausch zwischen allen Beteiligten an. Eine Fülle unterschiedlicher Regelungen und Vereinbarungen sowie eine heterogene IT-Landschaft im Bereich der nichtpolizeilichen Gefahrenabwehr erschweren jedoch heute den Informationsaustausch.

Obwohl in Deutschland ausreichendes Hilfeleistungspotenzial vorhanden ist, besteht die Gefahr, dass bei einer großflächigen Gefahrenlage die verfügbaren Hilfeleistungspotenziale nicht immer effizient eingesetzt werden. In der Vergangenheit wurden immer wieder Defizite im Bereich des Informationsmanagements insbesondere bei der Gewinnung und Aktualisierung eines umfassenden Lagebildes sowie bei der zeitgerechten Anforderung angemessener Ressourcen festgestellt.

Mit der Einführung des web-basierten deutschen Notfallvorsorge-Informationssystems (deNIS IIplus) und der Anbindung aller Lagezentren der Bundesressorts sowie der Lagezentren der Innenministerien der Länder hat das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ein Netzwerk auf der oberen und obersten Verwaltungsebene geschaffen. Hierdurch wird das Informationsmanagement im Hinblick auf die Lagedarstellung, das Ressourcenmanagement und das Meldewesen zwischen allen angeschlossenen Nutzern erheblich beschleunigt.

Die Einbeziehung weiterer Akteure – vor allem auf der mittleren und unteren Ebene der Gefahrenabwehr – ist jedoch, nicht zuletzt vor dem Hintergrund der europäischen Integration, notwendig.

Bei großflächigen Gefahrenlagen nehmen Kommunikation und Interaktion zwischen allen Beteiligten in einem erheblichen Umfang zu. Die Verantwortlichen der Gefahrenabwehr müssen daher neue Instrumente finden, um das Informationsmanagement zu verbessern. Dienste- bzw. serviceorientierte Architekturen bieten hierbei die Option, den Datenaustausches zwischen unterschiedlichen Krisenmanagementsystemen zu erleichtern sowie die Integration von Sensordaten aus Gefahrenerfassungssystemen zu ermöglichen.

Die Möglichkeiten der Informationstechnik und der elektronischen Vernetzungen müssen daher besser genutzt werden, um den neuen Herausforderungen gewachsen zu sein.

Es ist daher zu klären, welche Voraussetzungen geschaffen werden müssen, um das Management bei außergewöhnlichen Gefahren- und Schadenlagen zu verbessern. Das vorliegende Dokument des BITKOM analysiert treffend die Defizite der aktuellen Situation und zeigt technische sowie auch organisatorische Lösungsmöglichkeiten auf.

4 Technologische Innovationen nutzen

4.1 Technische Interoperabilität der IT-Architektur

Die Forderungen nach schnellen und flexiblen Reaktionsmöglichkeiten bei gleichzeitiger Sicherheit der Informationen führt zur Veränderung von Prinzipien und Methoden für die Architektur von Anwendungen:

Die serviceorientierte Netzwerk- und Anwendungsarchitektur (SONA/ SOA) zeichnet sich durch 3 Grundprinzipien aus:

- Logische und physikalische Trennung der Geschäftslogik von der Präsentationslogik
- Aufspaltung der Geschäftslogik in unabhängige Einzelmodule bzw. Dienste
- Kapselung der Funktionalität bzw. Implementierung der einzelnen Services über definierte Schnittstellen

Grundprinzipien der serviceorientierten Netzwerk- und Anwendungsarchitektur sind:

- Service-Beschreibung (Welche Dienste/Services stehen im Netz zur Verfügung?)
- Dienste-Aufruf (wie können solche Dienste genutzt werden?)
- Integration von verschiedenen Services zu Verbundanwendungen
- Definition von Geschäftsprozessen, die regelbasiert und ereignisgesteuert die Inanspruchnahme von Diensten/Services regeln.

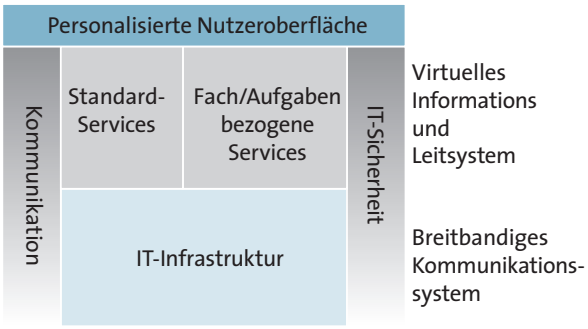

Abbildung 2: Service-orientierte Architektur

4.2 IT-Infrastruktur (einschl. Integration von Sensoren)

Netzinfrastruktur IP-Netz

Der aktuelle Stand der Kommunikationstechnologie sind heute IP-basierte Infrastrukturen. Diese bilden Sprache, Video und Daten auf einer Netzarchitektur ab. Eine solche Infrastruktur ist dienstunabhängig und stellt durch die standardmäßigen Funktionen bereits auf der untersten Ebene die geforderte Flexibilität zur Verfügung. Mit Hilfe dieser Technologie lässt sich sowohl eine Priorisierung von Services als auch eine flexible Bandbreitennutzung ermöglichen.

Mobilität

Durch die Integration von mobilen Übertragungstechniken (TETRA, GSM, UMTS, WLAN und WiMAX) werden die im IP-Festnetz bereitgestellten Möglichkeiten mit unterschiedlichen Bandbreiten auch für die mobile Nutzung zur Verfügung gestellt. Die heutige Generation der Endgeräte (Telefon, Handheld, Palmtop, Laptop, etc.) setzt dabei auf die IP-Technologie, so dass die Integration einfach zu realisieren ist. Auch Sicherheitsforderungen können damit durchgängig implementiert werden.

Entscheidend ist hier die logische Trennung zwischen der Übertragungstechnologie und den auf den Endgeräten vorhandenen Applikationen. Nur so kann sichergestellt werden, dass in Zukunft die Applikationen und Übertragungsmedien unabhängig voneinander weiterentwickelt werden können. Diese Unabhängigkeit führt dazu, dass während eines Krisen- und Katastrophenfalls nicht jede beteiligte Organisation ihre eigene Kommunikationsinfrastruktur aufbauen muss, sondern überflüssige Redundanzen verhindert werden und eine durchgängige Kommunikation sichergestellt werden kann.

Der Einsatz des Digitalfunks der BOS auf Basis der TETRA-Technologie wird hier langfristig unterstützen. Durch den Einsatz von dynamisch gebildeten Funkgruppen wird es den Einsatzkräften zukünftig einfacher gelingen, sich den aktuell gegebenen Situationen anzupassen. Bei der Bildung der Funkgruppen können vom Dispatcher Berechtigungen und Prioritäten verwaltet werden, die den Funkverkehr entflechten und strukturieren.

Gleichzeitig wird die endliche Ressource Bandbreite durch den Bündeleffekt optimal genutzt. Standardmeldungen lassen sich als Text (SDS[1]) übertragen, um den Sprechfunk zu entlasten.

Gleichzeitig ermöglichen verlegbare und mobile Ad-Hoc-Netze die schnelle, sichere und zuverlässige Einrichtung von Lagezentren einschließlich der Anbindung an die zentralen Verfahren. Einsatzkräften ist es durch den spontanen Netzeintritt möglich, sich bereits während der Anfahrt zum Einsatzort in die Lage einzuarbeiten. Dies führt zu einem wesentlichen Zeitvorteil und somit zu einer höheren Effizienz.

Sicherlich stellen diese Punkte heute im Alltag eine beherrschbare Aufgabe dar, da im vertrauten Einsatzgebiet Migrationslösungen rechtzeitig geplant und geschaffen werden können. Im Katastrophenfall jedoch bleibt meist nur wenig Zeit, sich zunächst klar zu werden, welche Organisation welchen technologischen Stand mitbringt, und wie hier spontan die Kommunikationsmittel sinnvoll zusammengeschaltet werden können.

1 SDS: Short Data Services, SMS-Dienst Bündelfunk

Sensordaten

Es ist erkennbar, dass zukünftig die Nutzung von Sensordaten durch Nutzer immer wichtiger wird. Hierfür existieren bereits heute zahlreiche Anwendungen: Verfolgung von gefährlichen Gütern oder auch Überwachung von Einsatzteams im Gefahrenbereich. Die Verknüpfung von Sensor- und Geodaten liefert zusätzliche Erkenntnisse über die Einsatzlage.

Sicherheit

Als grundlegende Sicherheit auf Netzebene kann das vorhandene IP-Sec-Protokoll genutzt werden, um darauf aufbauend VPN-Netze (Virtual private network) einzurichten. Ergänzend dazu muss der sichere Zugang zum Netz sichergestellt werden. Dazu dient eine Public Key Infrastructure (PKI) als elektronischer Identitätsnachweis auf Basis hochwertiger Schlüsselmittel und kryptographischer Verfahren. Damit kann ein rollen- und aufgabenorientierter Zugriff auf Services und Informationen sichergestellt werden.

4.3 Virtuelles Informations- und Leitsystem

Kommunikation

Kommunikation umfasst nicht nur den gemeinsamen Zugriff auf Daten in einem Anwendungssystem. Kommunikation beginnt mit Sprachkommunikation zwischen den eingesetzten Kräften und weiteren Behörden und Organisationen im Hintergrund. Gleichzeitig können die üblichen Kommunikationsmittel wie Fax oder E-Mail in die Arbeit integriert werden. Verschiedene Kommunikationskanäle werden im Zugang und in der Bearbeitung vereinheitlicht.

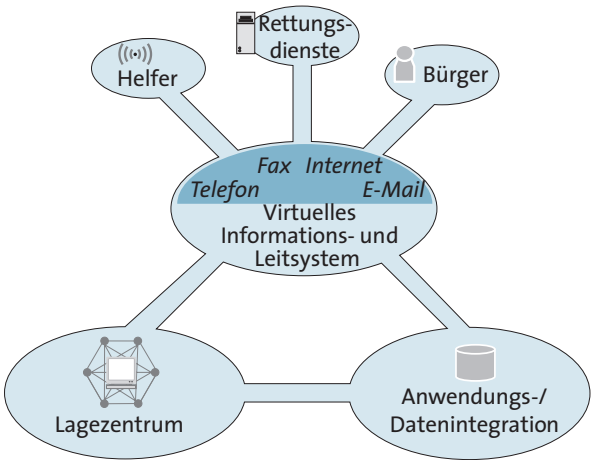

Abbildung 3: Virtuelles Informations- und Leitsystem

Integrierte Kommunikation

Ein IP-basiertes System ermöglicht es, alle Kommunikationskanäle in Applikationen und Prozesse zu integrieren. Dadurch ergeben sich insbesondere folgende Vorteile:

- Integration aller Informationen (Daten, Sprachkommunikation) in der personalisierten Applikationsumgebung des Nutzers („Unified Communications“).
- Erreichbarkeit von zuständigen Kontaktpersonen unabhängig vom verwendeten Medium (Mail, Telefon, Funk, ...).
- Vermeidung von Medienbrüchen durch konsequente, integrierte elektronische Verarbeitung.
- Vereinfachte, automatische, medienübergreifende Dokumentation von Abläufen.

Gemeinsame Lagebearbeitung

Zur schnellen und effektiven Lagebeurteilung über Standorte hinweg ist eine gemeinsame Arbeits- und Kommunikationsumgebung sinnvoll, die flexibel mit den jeweils vorhandenen Kommunikationskanälen bedient werden kann. Hierbei können zusätzlich Applikationen gemeinsam bedient und Live-Videodaten (z.B. vom Einsatzort) den Teilnehmern zur Verfügung gestellt werden. Dabei nutzt jeder Teilnehmer die Medien, die ihm an seinem Standort aktuell zur Verfügung stehen (z.B. nur Internetzugang, nur Sprache oder Sprache, Daten und Video). Die Lösung wird zentral als Dienst im IP Netzwerk bereitgestellt und kann somit von verschiedenen Stellen parallel genutzt werden. Die Einführung des Digitalfunks alleine wird hier nicht reichen, da dieser in seiner momentanen Ausbaustufe aufgrund beschränkter Bandbreite nur bedingt die Fähigkeit zur Übertragung von hochauflösenden Videodaten ermöglicht.

Diese gemeinsame Kommunikationsplattform ermöglicht es, Informationen aus verschiedenen Quellen gemeinsam zu sichten, zu beurteilen, Entscheidungen zu treffen und umzusetzen.

Standard-Service Auftragssteuerung und Workflow

Jede Organisationseinheit benötigt die Funktion „Auftragssteuerung“, um damit aus der Leitstelle/Leitzentrale heraus die eigenen Kräfte zielgerichtet führen zu können. Die möglichen Eskalations- und Entscheidungswege innerhalb und zwischen den einzelnen Beteiligten sind durch einen durchgängigen elektronischen Workflow zu unterstützen.

Fachservice Fusionierung von Informationen

Werkzeuge zur Unterstützung der Zusammenarbeit, wie „Meldungsaustausch“, „gemeinsamer Kalender mit Belegung gemeinsamer Betriebsmittel“, „Konferenzschaltungen für Lagebesprechungen mit gemeinsamen Bildschirm“, „Verteilung von Sprachnachrichten (Voice Messaging)“ und „gemeinsame Informationsablage“ sind wichtige Werkzeuge für Organisationen im Bereich der Inneren Sicherheit. Sie stellen Methoden und Mittel zur Vereinfachung der Zusammenarbeit zwischen

verschiedenen Gruppen von Nutzern, vor allem über Organisationsgrenzen hinweg, zur Verfügung.

Fachservice Suche in Informationen

Durch Suchwerkzeuge können heute inhaltliche Volltextrecherchen realisiert werden. Dadurch kann in großen unstrukturierten Datenbeständen schnell und effektiv nach den benötigten Informationen gesucht werden. So können relevante Informationen rechtzeitig in den Entscheidungsprozess mit einfließen.

Das Konzept des gemeinsamen operationellen Lagebildes, welches eine gemeinsame Sicht für alle operationellen Nutzer bereitstellt, erfordert das Verschmelzen von Daten verschiedener Quellen. Die Verbindung von positions- und sensorbasierten Informationen mit den Sachdaten bzw. erfassten oder gemeldeten Informationen ist eine Schlüsselkomponente, um ein gemeinsames Bild aufzubauen. Diese Informationen müssen so gestaltet sein, dass sie sowohl in der „Operationszentrale“ als auch auf den mobilen Endgeräten am Einsatzort nutzbar sind.

IT-Sicherheit

Eine umfassende Sicherheitsstrategie wird mögliche Bedrohungen identifizieren. Innerhalb einer Infrastruktur lässt sich „Sicherheit“ noch einmal kategorisieren:

- Technische Sicherheit – Sicherung der physischen und virtuellen Netzwerk-Verknüpfungen zwischen Elementen der Infrastruktur, z.B. von Clients zu den Servern.
- Anwender Authentifizierung – stellt sicher, dass die Anwender auch die sind, die sie vorzugeben scheinen.
- Zugriffssicherheit – welche Benutzer haben Zugriff auf welche Daten und Informationen und wozu?
- Daten und Informationssicherheit – hier werden Funktionalitäten benötigt, um die Kritikalität der Informations- und Datenelemente zu klassifizieren.
- Verarbeitungssicherheit – Schutz vor unautorisiertem Zugriff, Schadfunktionalitäten sowie Modifikation/Manipulation von Verarbeitungsschritten und Transaktionen.

Identitäts-Management

Die Fähigkeit, die Identität der Anwender festzulegen, beizubehalten und Berechtigungen zentral entziehen zu können, ist eine Schlüsselanforderung an Systeme mit sensitivem Datenbestand. Dies erfordert strenge Zugriffskontrollen, z. B. die Berechtigung der Anwender eines Systems (z.B. Polizei, Feuerwehr) Informationen auf einem anderen System nutzen zu dürfen.

4.4 Organisatorische Interoperabilität

Mit der Einführung des web-basierten deNIS IIplus im Gemeinsamen Melde- und Lagezentrum des Bundes (GMLZ) und der Anbindung von über 100 Nutzern von Bund, Ländern und Hilfsorganisationen wurde seitens des Bundes Vorsorge getroffen, dass zumindest im Hinblick auf die Lagedarstellung, das Ressourcenmanagement und das Meldewesen der elektronische Informationsaustausch zwischen allen angeschlossenen Nutzern auf Stabsebene erheblich beschleunigt werden kann.

Für ein effizientes Krisenmanagement reicht eine Beschleunigung des Informationsaustausches allein nicht aus; vielmehr muss sichergestellt werden, dass alle in einem Netzwerk zusammenwirkenden Systeme dieselben Daten auch gleichartig zu interpretieren erlauben. Hierzu muss die semantische Interoperabilität der Daten und Systeme gewährleistet werden.

Dies gilt es zu entwickeln, unter Einbindung bestehender Standardisierungsbestrebungen seitens des Beauftragen der Bundesregierung für Informationstechnik, der OSCI[1]-Leitstelle sowie Vertretern der BOS und entsprechender IT-Hersteller.

Angesichts der geographischen und politischen Lage Deutschlands ist eine europäische Einbettung zur Sicherstellung der Interoperabilität bei grenzüberschreitenden Krisen angezeigt.

Effizienzgewinn durch Interoperabilität

Organisatorische Interoperabilität ist der Schlüssel zu einer Verbesserung des Katastrophenschutzsystems Deutschlands. Dieses ist gekennzeichnet durch eine Vielzahl von öffentlichen, non-profit und privaten Organisationen, die abhängig vom jeweiligen Schadensszenario temporär und ad hoc zusammenarbeiten. Kritischer Erfolgsfaktor für die Bewältigung von Schadensfällen und damit der Rettung von Menschenleben ist der Faktor Zeit. Um auf Schadensfälle effektiver und effizienter als in der Vergangenheit reagieren zu können, müssen die Maßnahmen und Abläufe der beteiligten Organisationen möglichst verzahnt und synchronisiert ablaufen. Abstimmungen zu Verantwortlichkeiten und dem jeweiligen Hilfeleistungspotenzial zum Zeitpunkt einer eingetretenen Großschadenslage sind zeitaufwändig und könnten durch eine gesamtstaatliche Sicherheitsarchitektur, welche durch organisatorische Interoperabilität gekennzeichnet ist, deutlich reduziert werden.

Voraussetzungen für Interoperabilität

Voraussetzung für die organisatorische Interoperabilität ist die Einbindung möglichst aller am Katastrophenschutz beteiligten Organisationen in eine Gesamtarchitektur, die Organisation, Prozesse (und Fähigkeiten), Daten, Anwendungen und Informationstechnik umfasst. Eine wesentliche Komponente dieser Informationsarchitektur sind die Fähigkeiten, mit welchen einzelne Organisationen grundsätzlich einen Beitrag zur Bewältigung von spezifischen Schadenslagen leisten können. Eine zweite Komponente der Gesamtarchitektur besteht aus den Verfahren der Zusammenarbeit zwischen den Beteiligten. Um die schnelle Zusammenarbeit zu gewährleisten, müssen notwendige Organisations- und Informationsschnittstellen z.B. mit Hilfe von Referenzprozessen definiert und konkretisiert sein. Die beiden Komponenten Fähigkeiten und organisatorische Schnittstellen sind Mindestbestandteil einer Gesamtarchitektur, die sich als Grundlage für die Entwicklung einer organisatorischen Interoperabilität eignet.

Über diese Mindestbestandteile hinaus sollten in weiteren Ausbaustufen ebenfalls aktuelle Daten über die Verfügbarkeit von Materialmengen und die Anzahl verfügbarer Personen, die einer bestimmten Fähigkeit zugeordnet sind, bereitgestellt werden. Voraussetzung hierfür ist die Schaffung der oben angesprochenen semantischen Operabilität. Die für das Lagebild der eigenen Ressourcen notwendigen Informationstechnologien gehören im industriellen Bereich mittlerweile zum Standard.

Methodischer Rahmen für Interoperabilität

Ausgehend von der Vielzahl existierender Notfallpläne in Deutschland, dürfte unser Land sehr gut vorbereitet sein für alternative Schadensereignisse. Notfallpläne liegen nicht nur „in den Schubladen“ von Ländern, Kreisen und Kommunen, den Hilfsorganisationen und Einrichtungen des Gesundheitswesens bereit, sondern vielfach auch bei privaten Unternehmen. Es gilt diese Pläne szenariobasiert zu harmonisieren und Synergieeffekte z.B. bei benachbarten Hilfsorganisationen zu nutzen.

Um die Interoperabilität innerhalb einer Organisation und über Organisationsgrenzen hinaus sicherzustellen hat sich das Enterprise Architecture Management (EAM) bewährt. Dabei wird mit der Definition der Ziele und der

1 Online Services Computer Inferface

übergreifenden Architekturvorstellung begonnen, um darauf aufbauend die erforderlichen (Geschäfts-)Prozesse zu modellieren. Daraus können die benötigten Organisationselemente in den einzelnen Organisationen abgeleitet werden. Parallel dazu werden die erforderlichen Daten identifiziert und in Datenmodellen dargestellt. Diese Sicht erlaubt nun die Ermittlung der benötigten Anwendungssysteme zur optimalen Unterstützung der Prozesse. Sind diese bekannt, kann die erforderliche Hardware (Server, Netze, mobile Komponenten, etc.) abgeleitet werden.

5 Empfehlungen

BITKOM empfiehlt den Sicherheitskräften und Hilfsorganisationen in Deutschland als Grundvoraussetzung für ein gemeinsames Krisen- und Katastrophenmanagement die „Interoperabilität“ (1) der vorhandenen Informationssysteme herzustellen. Dazu ist die Unterstützung der Wirtschaft und Wissenschaft erforderlich.

Um Interoperabilität herzustellen, sind Voraussetzungen auf drei Ebenen zu schaffen

- Organisatorische Interoperabilität mit der Abstimmung von Gesetzen, Regelungen und Prozessen.
- Semantische Interoperabilität mit der Vereinheitlichung von Datenstrukturen und (IT-)Diensten.
- Technische Interoperabilität mit der Standardisierung von Protokollen und technischen Schnittstellen.

BITKOM schlagt daher vor:

- Organisation
  Zur Herstellung der organisatorischen Interoperabilität ist zumindest für ausgewählte Szenarien eine Fähigkeits-Analyse und Bestimmung der organisatorischen Anforderungen, Anwendungsszenarien und Rahmenbedingungen für ein erfolgreiches Zusammenwirken durchzuführen.
- Inhalte (Semantik)
  Zur Erreichung der semantischen Interoperabilität ist eine Standardisierung der Inhalte für einen elektronischen Informationsaustausch durchzuführen. Hierzu sollte eine entsprechende Arbeitsgruppe eingerichtet werden, in der zwingend die Fachkompetenz der Anwender vertreten sein muss.
- Technologie
  Für die technische Interoperabiliät empfehlen wir, sich auf eine gemeinsame, herstellerunabhängige und offene IT-Architektur zu verständigen und darauf aufbauend eine integrierte und sichere IT-Infrastrukur für Sicherheitsanwendungen einzurichten.
  Hierbei ist zu berücksichtigen, dass sich Bund und Länder in der 2002 vereinbarten „Neuen Strategie zum Bevölkerungsschutz“ auf die gemeinsame Säule „deutsches Notfallvorsorge-Informationssystem“ (deNIS) verständigt haben.

Fazit

Die Voraussetzung zur Umsetzung der obengenannten technischen Interoperabilität liegen in Form von Hard- und Softwareprodukten sowie durch die Erfahrung und Leistungsfähigkeit kompetenter Unternehmen der ITK Branche vor. Die semantische Interoperabilität lässt sich durch eine Expertengruppe aus der Wirtschaft und den beteiligten Organisationen erarbeiten. Zur Erreichung der organisatorischen Interoperabilität ist vor allem der Wille, diese Herausforderung über den Rahmen von Zuständigkeitsfragen hinaus anzunehmen, erforderlich. Es besteht keine Notwendigkeit auf weitere Impulse zu warten. Eine Unterstützung dieser Ansätze durch effiziente Einsatzübungen kann die Interoperabilität weiter verbessern.

BITKOM steht für den Dialog zur Verfügung.

Danksagung

Das vorliegende Dokument konnte nur durch die engagierte Mitarbeit der Experten aus den Mitgliedsunternehmen erstellt werden. BITKOM bedankt sich daher an dieser Stelle insbesondere bei:

- Michael Bartsch, T-Systems Enterprise Services GmbH
- Stephan Koch, Steria Mummert Consulting AG
- Christian Koehler, IABG mbH
- Alexander Mayer, Cisco Systems GmbH
- Ralph Michel, IDS Scheer AG
- Werner Wirdemann, ORACLE Deutschland GmbH
- Jürgen Zender, CONET Solutions GmbH

sowie bei den restlichen Mitgliedern des Arbeitskreises Homeland Security.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org