Vernetzt für den Notfall

Autor(en): **Fuchs, Christian / Smit, Patrick**

Objekttyp: **Article**

Zeitschrift: **Bevölkerungsschutz : Zeitschrift für Risikoanalyse und Prävention, Planung und Ausbildung, Führung und Einsatz**

Band (Jahr): **4 (2011)**

Heft 9

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-357912

Nationale Alarmzentrale NAZ

Vernetzt für den Notfall

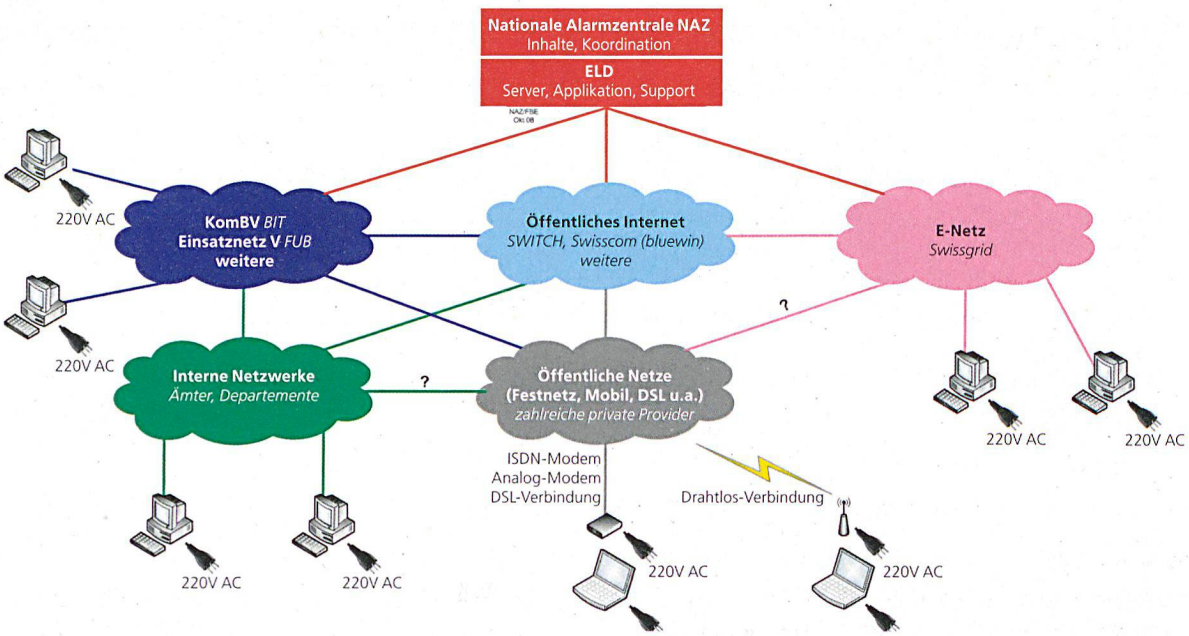
Bei der Bewältigung von Katastrophen und Notlagen ist die Vernetzung und der Dialog zwischen den verschiedenen Partnerorganisationen des Bevölkerungsschutzes entscheidend. Nur wenn die Kommunikation gewährleistet ist, können Lageinformationen ausgetauscht, Massnahmen angeordnet und koordiniert werden. Die NAZ setzt auf ein umfassendes Kontinuitätsmanagement, um die Verbindungen auch im Ereignisfall nicht abreissen zu lassen. Sichere Verbindungen bleiben aber eine grosse Herausforderung.

Von der Erfassung einer Gefahr durch eine Fachstelle bis zum Ergreifen von Schutzmassnahmen durch die Bevölkerung braucht es eine ganze Kette von Teil-Prozessen. Alle sind auf funktionierende Kommunikationskanäle angewiesen.

Im Bevölkerungsschutz werden zunehmend Szenarien und Ereignistypen diskutiert, die eine Zusammenarbeit zahlreicher Partnerorganisationen auf verschiedenen Stufen erfordern. Ob Pandemie, grossflächiger Stromausfall, schweres Erdbeben oder «schmutzige Bombe»: immer müssen die verschiedenen Führungsorgane und deren Partner sich untereinander vernetzen und Informationen austauschen. Zudem hat sich die Anzahl der Kommunikationsmittel genauso wie der involvierten Partner erhöht. Während früher die Telematik-Netze der PTT die Partner von Bund und Kantonen verbanden, werden heute diverse Kommunikationskanäle verschiedenster Anbieter genutzt. Funktionierende Verbindungen sind nicht nur wichtiger geworden, sondern auch komplexer.
Die NAZ kann dabei auf ihre Erfahrung im Bereich «Ereignisse mit erhöhter Radioaktivität» zurückgreifen. Hier ist schon seit Jahrzehnten eine gemeinsame Ereignisbewältigung von Bund und Kantonen vorgesehen: Bei einem Zwischenfall in einem Schweizer KKW kommen die Aufsichtsbehörde ENSI und der Kraftwerkbetreiber hinzu. Entsprechend wichtig ist die Kommunikation innerhalb und zwischen all diesen Organisationen.

Ausfallsicherheit verschiedener Systeme

Bereits 2002 führte die NAZ eine Umfrage bei den Betreibern von Kommunikationsnetzen durch, um die Ausfall-



Die NAZ stellt die Elektronische Lagedarstellung ELD über verschiedene Netze zur Verfügung, über die die Partnerorganisationen einen Zugang sicherstellen können. Die Illustration zeigt geplante und bereits realisierte Zugangsmöglichkeiten.

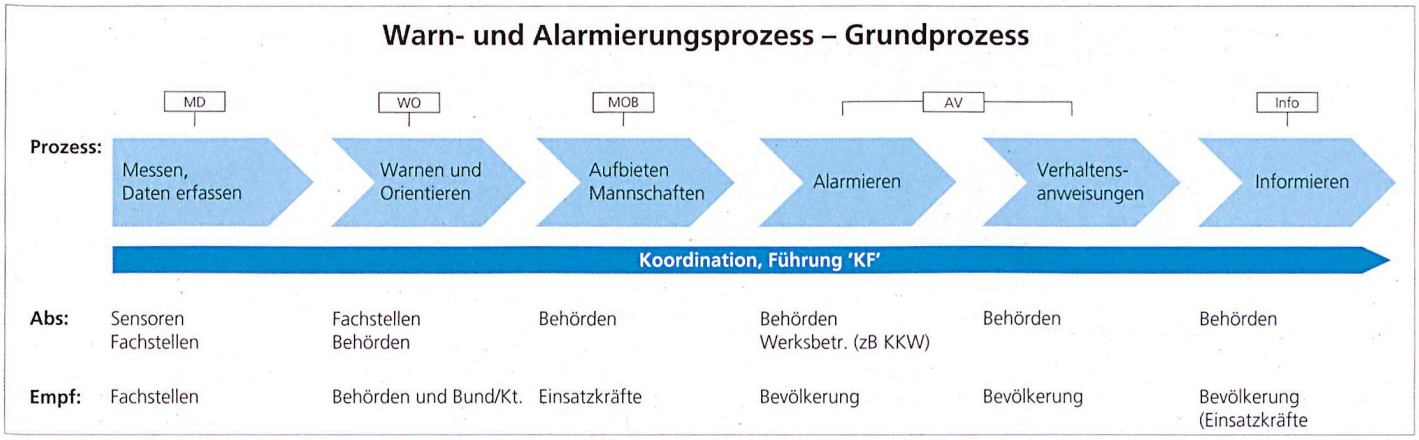
sicherheit verschiedener Systeme zu beurteilen, die bei der Ereignisbewältigung zum Einsatz gelangen. Dabei zeigte sich, dass insbesondere bei einem grossflächigen Stromausfall diverse Informatik- und Kommunikationssysteme sofort oder nach kurzer Zeit nicht mehr funktionieren würden. Dies betrifft beispielsweise die Mobiltelefonie und verwandte Systeme wie den mobilen Datenverkehr, der für die Datenübertragung zwischen den Messsonden und dem Datenzentrum eingesetzt wird. Als ziemlich ausfallsicher kann das Internet gelten – sofern der Benutzer über eine Informatikinfrastruktur mit einer funktionierenden Stromversorgung verfügt. Dies ist mit dem Grundkonstruktionsprinzip des Internets zu erklären: Bei einem Verbindungsausfall «sucht» das Datenpaket selbständig einen anderen, noch funktionierenden Weg zum Adressaten. Damit ist das Netz anderen Systemen überlegen. Als Anfang 2010 in Haiti die Erde bebte, brachen die wichtigsten Kommunikationsverbindungen ins Ausland sofort ab. Auch Tage nach dem Beben waren internationale Verbindungen über das Fest- und Mobilnetz nicht möglich. Über Internettelefondienste und den Microblog-Dienst Twitter gelang es jedoch, Meldungen über die Situation und die angerichteten Schäden zu verbreiten. Internationale Hilfsorganisationen nutzten solche Nachrichten, um eine Übersicht über die Lage zu erlangen. Auch nach den Anschlägen vom 11. September 2001 fiel das Internet in Manhattan im Gegensatz zur Telefonie praktisch nicht aus. Allerdings wurde eine Überlastung bestimmter Websites festgestellt, die dann nicht mehr erreicht wurden.

Der Bericht «Optimierung Kommunikation EOR»

Der Leitende Ausschuss Radioaktivität will garantiert haben, dass die Organisationen, die an der Bewältigung eines Ereignisses mit erhöhter Radioaktivität beteiligt sind, auch künftig untereinander sicher kommunizieren können. Deshalb liess er die Bedürfnisse bei den Verbindungen innerhalb der Einsatzorganisation bei erhöhter Radioaktivität EOR systematisch erfassen. Als Grundlage diente die «Kommunikationskette», die im Rahmen der Optimierung der Warnung und Alarmierung bei Naturgefahren (OWARNA) definiert wurde. Diese Kette zeigt auf, wo die Kommunikation funktionieren muss, damit die Bevölkerung und ihre Lebensgrundlagen vor Gefahren und deren Auswirkungen wirksam geschützt werden können. Wie jede Kette ist sie so stark wie das schwächste Glied: Bricht die Kommunikation irgendwo ab, können alle weiteren Bereiche nicht mehr befriedigend bearbeitet werden.
Der Bericht zeigt auf, wie weitreichend die Bedürfnisse innerhalb der EOR sind. Sichere Verbindungen braucht es nicht nur in der Telefonkonferenz zwischen den Partnerorganisationen, es braucht sie genauso zur Datenübermittlung der stationären und mobilen Radioaktivitätssonden im Feld, zum ferngesteuerten Auslösen der Sirenen, zum Aufbieten der Mannschaften und zum Verbreiten von Radiodurchsagen, welche der Bevölkerung Verhaltensanweisungen erteilen.

Erfolgsfaktor Kontinuitätsmanagement

Für den Fall, dass kritische Kommunikationssysteme nicht zur Verfügung stehen, heisst das Zauberwort Kontinuitätsmanagement (bekannt auch unter dem englischen



Begriff BCM, Business Continuity Management). Es umfasst Planungen, um die Handlungsfähigkeit zu bewahren – etwa indem auf ein anderes Kommunikationsmittel ausgewichen wird oder das Personal für entsprechende Massnahmen geschult wird. Es ist entscheidend, dass alle Partner Planungen vornehmen und Vorkehrungen treffen sowie ihre Massnahmen im Kontinuitätsmanagement untereinander abstimmen.

Die NAZ setzt verschiedene Konzepte des Kontinuitätsmanagements ein, um auch unter erschwerten Bedingungen arbeiten zu können. So rücken die NAZ-Piketts beispielsweise selbständig ein, wenn sie bei einem grossflächigen Stromausfall oder nach einem starken Erdbeben die NAZ nicht erreichen können. Damit steht auch Personal zur Verfügung, wenn die Pager nicht mehr funktionieren. Wo immer möglich schafft die NAZ Redundanzen, um beim Ausfall eines Systems auf ein anderes zurückgreifen zu können. Gegenwärtig wird beispielsweise das Bündelfunksystem POLYCOM in die Prozesse der Alarmstelle NAZ und des taktischen Piketts eingeführt. Dieses Sicherheitsnetz soll die bestehenden telefonischen Kanäle nicht generell ersetzen; vielmehr soll eine Rückfallebene bestehen, falls die im Alltag üblichen Kommunikationssysteme versagen.

ELD: Redundanz über verschiedene Netze

Für die Erstellung einer Lageübersicht und die Zusammenarbeit mit ihren Partnern setzt die NAZ auf eine internetbasierte Lösung, die geschützte Informationsplattform ELD (Elektronische Lagedarstellung). Die NAZ als Betreiberin des Systems stellt dabei den Betrieb der hochverfügbaren Server sicher, auf denen diese Plattform installiert ist. Dafür nutzt sie verschiedene Sicherheitssysteme und redundante Server mit hoher Kapazität. Die NAZ setzt zudem Dateiformate ein, die möglichst wenig Datenverkehr verursachen und das System nicht überlasten sollen.

Um noch mehr Sicherheit zu gewinnen, wird die ELD den Partnerorganisationen aber nicht nur über das Internet, sondern auch über andere Netze zugänglich gemacht, etwa über das interne Netz der Bundesverwaltung. Damit können die Partnerorganisationen eigene Redundanzen und ein eigenes Kontinuitätsmanagement sicherstellen. Fällt ein Netzzugang aus, kann über einen anderen Zugang oder über ein anderes Netz versucht werden, die Verbindung wieder herzustellen.

Diese Philosophie trägt dem Gedanken Rechnung, dass die NAZ über ein äusserst heterogenes Partnernetz verfügt. Nicht alle Partner haben etwa Zugang auf das hochverfügbare Einsatznetz der Armee. Einige Partner haben dezentrale Führungsstandorte, kaum Ressourcen für ausfallsichere Verbindungen oder sie befinden sich im Ausland. Partnerorganisationen, die nur Zugang zum Internet haben, setzen am besten zwei unabhängige Zugangspfade ein, etwa über zwei verschiedene Kabelnetze. Wichtig ist, dass jede Organisation nach Möglichkeit dazu beiträgt, dass die Verbindung nicht abreisst.

Konstante Herausfordernung: ausfallsichere Netze

Die Sicherstellung von Verbindungen zu allen Verbundpartnern bleibt eine ständige Herausforderung, nicht nur für die NAZ, sondern für alle Einsatzorganisationen und Partner im Bevölkerungsschutz. Der Erfolg der Einsatzbewältigung hängt wesentlich davon ab, dass alle beteiligten Partner in ihrem Bereich Redundanzen schaffen und über ein umfassendes Kontinuitätsmanagement verfügen. Auch bei der NAZ besteht diesbezüglich Handlungsbedarf. Sie beteiligt sich darum aktiv an den Projekten des BABS, die hier Verbesserungen erzielen sollen.

Christian Fuchs
Chef Information Nationale Alarmzentrale NAZ, BABS

Patrick Smit
Chef Einsatz Nationale Alarmzentrale NAZ, BABS