



Professionelle mobile Kommunikationsdienste für Kritische Infrastrukturen

Mit Sicherheit mobil kommunizieren

Die mobile Vermittlung von Informationen wird heute gerne als Selbstverständlichkeit angesehen. Dennoch zeigt sich in krisenhaften Situationen, dass die vertrauten und häufig genutzten Kommunikationsdienste ausgesprochen störanfällig sind. Gerade bei Großschadensereignissen, Naturkatastrophen, terroristischen Anschlägen oder in Spitzenbelastungszeiten kommt es immer wieder zum folgenschweren Ausfall der nicht- oder semiprofessionellen mobilen Kommunikationsnetze. Um so wichtiger sind ergänzende Mobilfunktechnologien wie Funkruf. Gerade professioneller Funkruf erlaubt es im Sinne von Zweitalarmierungsweg bzw. Rückfallebene auch im Ernstfall weiterhin zuverlässig mobil kommunizieren zu können.

Für Kritische Infrastrukturen bietet e*Message folgende drei professionelle Kommunikationsdienste:

e*BOS: Die exklusive Alarmierungslösung für Behörden und Organisationen mit Sicherheitsaufgaben (BOS).

e*Cityruf: Der klassische Paging Service für Profis in Unternehmen, Institutionen und Behörden.

e*Dispatch: Besondere Kompetenz beweist e*Message in Berlin-Brandenburg. Das Unternehmen hat als einziger Telekommunikationsanbieter seinen Hauptsitz in der Bundeshauptstadt. Mit e*Dispatch bietet e*Message im Großraum Berlin zusätzlich einen leistungsfähigen Bündelfunkdienst für Sprach- und Datenkommunikation.

Mit allen drei mobilen Services kann den besonderen Herausforderungen und Sicherheitsanforderungen der Hauptstadtregion entsprochen werden.

Kritische Infrastrukturen als Achillesferse moderner Gesellschaften

Die Funktionsfähigkeit von technisch hochentwickelten Gesellschaften wie der Bundesrepublik hängt vital von den Informations- und Kommunikationsnetzen ab. Kommt es bei „Kritischen Infrastrukturen“ zu massiven Störungen, kann dies folgenschwere Kettenreaktionen auslösen. Da die Risiken allzu häufig unterschätzt werden, kümmert sich das Bundesamt für Sicherheit und Informationstechnik (BSI) um Aufklärung. Dabei werden gezielt öffentliche Bedarfsträger in Bund, Ländern und Kommunen sowie Unternehmen angesprochen.

Das BSI definiert als „Kritische Infrastrukturen“ Organisationen und Einrichtungen, „bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen“ eintreten würden. Konkret zählen laut BSI zu Infrastrukturen mit kritischen, von IT abhängigen Systemen u.a. die Bereiche Transport und Verkehr, Energie (so sind herkömmliche mobile Kommunikationsdienste auf Stromversorgung angewiesen), Informationstechnik und Telekommunikation, Finanz-, Geld- und Versicherungswesen (mit IT-

abhängigen Dienstleistungen), Versorgung (von Wasser bis Gesundheits- und Rettungswesen), Behörden, Verwaltung und Justiz. Nur wenn all diese Bereiche ohne wesentliche Störungen funktionieren und reibungslos zusammenwirken, ist das Gemeinwesen dauerhaft lebensfähig.

Kritische Infrastrukturen auch bei Wirtschaftsunternehmen

Kritische Infrastrukturen gibt es nicht nur im großen Maßstab, sondern ebenso bezogen auf Wirtschaftsunternehmen. Auch hier können Störungen an neuralgischen Stellen zu deutlichen ökonomischen Schäden führen. Das BSI spricht beispielsweise von maximal zwei Wochen, die in den finanziellen Kollaps führen. Heutige Störungen sind eher von kurzer Dauer, können aber bereits zu erheblichen Problemen in der mobilen Kommunikation führen, wie die Übersicht im Anhang zeigt.

Einmal mehr ist hier die sichere und schnelle Vermittlung von Informationen einer besonderen Gefährdung ausgesetzt. Trotzdem zeigen Umfragen (z.B. des BSI), dass sich nur wenige Unternehmen der Risiken bewusst sind. Zwar gaben gegenüber dem BSI 98 Prozent der Befragten an, funktionierende IT-Systeme seien für den Arbeitsablauf sehr wichtig, aber selbst unter den IT-Experten hielten rund 80 Prozent ihre eigene Organisation für wenig störanfällig. „Diese Fehleinschätzung hinsichtlich der eigenen Betroffenheit zeigt ein weiteres Problem: Unkenntnis!“ So die Interpretation des Leiters des BSI, Dr. Udo Helmbrecht, in einem Vortrag auf dem Security Kongress im November 2004. Denn nicht nur das Absichern eines Servers ist von zentraler Bedeutung, sondern auch eine zuverlässig funktionierende Rückfallebene bei professionellen mobilen Kommunikationsdiensten.

Wie rasch gerade im Zusammenspiel der Infrastrukturbereiche Störungen – im Sinne des Domino-Effekts – eskalieren können, erklärt Dr. Helmbrecht an einem Beispiel: „In der Schweiz fällt ein Baum um und in ganz Italien geht das Licht aus, so wie im September 2003 tatsächlich geschehen. Kleine Ursache, große Wirkung.“ Eine Kettenreaktion lässt sich dann so beschreiben: „Der Stromausfall kann zum Ausfall des Telefonnetzes führen, alle Betroffenen greifen auf ihr Mobiltelefon zurück. Wenn dadurch das Mobilfunknetz in einer Region nicht ebenfalls komplett zusammenbricht, sind irgendwann die Akkus leer – und spätestens dann geht nicht mehr viel.“

Gerade herkömmliche Kommunikationsdienste sind hinsichtlich Stromversorgung immer anfällig. Dies zeigen auch die Erfahrungen im Ohrekreis (Sachsen-Anhalt). Hier hat die digitale Alarmierung mit dem e*BOS-System von e*Message ihre erste „Feuerprobe“ beim Orkan Kyrill im Januar 2007 bestanden: Als flächendeckend der Strom und teilweise auch Handynetze ausfielen, die Sirenen nicht funktionierten und zu allem Überfluss ein Blitz in einen Sendemast einschlug, zeigte sich e*BOS von all dem unbeeindruckt – die Leitstelle konnte die Einsatzkräfte jederzeit erreichen und effektiv koordinieren.

Ähnliche Kettenreaktionen gibt es auch in betrieblichen Strukturen. Schon die Tatsache, dass der Außendienst nicht erreichbar ist oder Lkws unzureichend dirigiert werden und ihre Ware nicht just-in-time beim Kunden anliefern, können zu folgenschweren Verwerfungen führen. Mobile Kommunikationsdienste zählen immer dann zu den Kritischen Infrastrukturen, wenn ihr Ausfall entscheidende Abläufe in Produktion/Verwaltung/Gesellschaft intensiv und nachhaltig negativ beeinflusst. Ursachen für den Ausfall der Mobilkommunikation können unterschiedlicher Art sein

– Stromausfälle, Katastrophen, Unfälle oder auch Anschläge – alles vorstellbare und keineswegs abwegige Szenarien, nicht nur für den Großraum Berlin-Brandenburg.

Die IT-Sicherheit und die Absicherung professioneller mobiler Informationsdienste ist somit für Unternehmen mindestens ebenso wichtig wie für vergleichbare Modelle im Gemeinwesen. Wobei ein Grund für die oft allzu stiefmütterliche Behandlung dieses Themas in den Investitionen begründet liegen mag. Denn zunächst kostet die Absicherung potenziell kritischer Infrastrukturen Geld. Ein Investment, das sich nicht sofort bezahlt macht und deshalb gerne zurückgestellt wird. Dr. Helmbrecht bringt das Dilemma bildhaft auf den Punkt: „Aber Vorsorge muss vor dem Eintritt eines Schadens erfolgen. Wer ins Wasser fällt und nicht schwimmen kann, der kann es auch dann nicht mehr lernen.“

Anforderungen an professionelle mobile Kommunikationsdienste

Moderne Kommunikationsnetze können nach dem Grad ihrer Professionalität unterschieden werden. Haben die übervermittelten Botschaften primär privaten Charakter, dann kann die Kommunikation als nichtprofessionell qualifiziert werden. Vermischen sich private und „professionelle“ Inhalte bzw. Nutzer (wie beim Handy), kann man von semiprofessionellen Systemen sprechen. In beiden Fällen sollte die Kommunikation möglichst immer funktionieren, muss aber nicht.

Kommunikationsnetze, die primär der Vermittlung nichtprivater Informationen dienen, gehören in die professionelle Kategorie. In dem Fall muss mobile Kommunikation immer funktionieren. Ein klassischer Vertreter dieser professionellen Kommunikationsdienste ist der Funkruf.

Dass diese Unterscheidung wichtig ist, wird sofort klar, wenn die Konsequenzen in Betracht gezogen werden. Während bei rein privat genutzten Medien technische Ausfälle zwar unerwünscht, aber in Grenzen tolerierbar sind, müssen professionelle Kommunikationsdienste einen außerordentlich hohen Grad an Zuverlässigkeit aufweisen. Schließlich hängt von ihrer reibungslosen Funktion auch und gerade unter extremen Bedingungen das Funktionieren komplexer, oft lebenswichtiger Infrastrukturen ab. Dabei reicht das Spektrum im öffentlichen Bereich vom Rettungswesen bis zum Katastrophenschutz, bei Firmen und Unternehmen vom Werksschutz bis hin zur Logistik.

Etablierung von Redundanzen und Rückfallebenen

Daraus resultierend gibt es bei der Entscheidung für Kommunikationsnetze eine klare Maxime: Je professioneller das Anforderungsprofil ist, desto zuverlässiger und krisenresistenter muss die Technik sein. Zudem bedarf es redundanter Systeme, die Informationsvermittlung auch dann sicherstellen, wenn ein Medium ausgefallen ist.

An Vorbildern für diese Methode hat es keinen Mangel. Dass der Mensch über zwei Nieren verfügt, ist eine kluge Vorsichtsmaßnahme: Fällt eine aus, kann die andere die Entgiftung des Körpers vollständig übernehmen. In der Natur gibt es viele Beispiele für redundante (lat. redundare = im Überfluss vorhandene) Lösungen, die durch mehrfaches Vorhandensein von „Komponenten“ die Ausfallsicherheit erhöhen. In der Technik wird diese Strategie überall dort adaptiert, wo eine Störung zum folgenschweren Totalausfall führen könnte. So sind in der Raumfahrt oder im

Luftverkehr zahlreiche Systeme redundant ausgelegt. Gleiches gilt für Kernkraftwerke oder die Stromversorgung von Krankenhäusern.

Aber gerade der IT-Bereich hat hier deutlich Nachholbedarf. Zwar ist vieles doppelt ausgelegt, wie zum Beispiel Server, aber die verantwortlichen Kommunikationsleiter denken selten an Mobilfunk. Das so genannte „Mobile Security Konzept“ wird oft ausschließlich im Sinne von Mithören, Virenangriffen und Missbrauch gedacht. Dass aber der Ausfall von professionellen Kommunikationsdiensten zu erheblichen Verwerfungen mit messbaren ökonomischen Schäden führen kann, ist oft nicht im Blickfeld der handelnden Personen.

„Sprachlose“ Verwunderung in London

Entscheidend für den Einsatz entsprechender Lösungen ist die Einschätzung des Risikos bei einem technischen Ausfall. Und genau hier läuft der Mensch Gefahr, sich subjektiv der Illusion einer vermeintlichen Sicherheit hinzugeben. Was tagtäglich ohne Probleme funktioniert, wird allzu gern als potenzielle Gefahrenquelle ignoriert. Warnungen von Experten verhallen ungehört. Und es bedarf erst katastrophaler Ereignisse, um darauf aufmerksam zu werden.

Ganz besonders gilt diese Einschätzung für die Kommunikation. Im Zeitalter von Internet und mobiler Kommunikationssysteme ist der sekundenschnelle Austausch von Informationen eine Selbstverständlichkeit. Um so größer die „sprachlose“ Verwunderung, wenn es plötzlich mit der Kommunikation nicht mehr klappt. Und erst dann zeigen sich die womöglich fatalen Konsequenzen. So geschehen in London beim Zusammenbruch der örtlichen Festnetz- und Mobiltelefonnetze nach den Bombenanschlägen vom 7. Juli 2005. Nur wer über den professionellen Kommunikationsdienst TETRA verfügte (Terrestrial Trunked Radio), war über den digitalen Bündelfunk erreichbar. Zwar wären genug Rettungskräfte vorhanden gewesen, nur gelang es nicht, diese effizient zu koordinieren. Laut „Telegraph“, der größten britischen Tageszeitung, seien die Rettungseinsätze „katastrophal“ verlaufen. „Wir mussten feststellen“, resümiert Martin Flaherty vom London Ambulance Services, „dass wir zu abhängig von Mobiltelefonen geworden sind. Jetzt ist klar, dass wir uns im Ernstfall nicht darauf verlassen können.“ Für den Director of Operations stand schnell fest, dass es zur Absicherung eines Backup-Systems bedurfte. Wie die City of London Police entschied sich auch der Rettungsdienst nach diesen Ereignissen für ein Paging-Alarmierungssystem.

Netzausfälle: Vielfältige Ursachen

Die Erfahrungen der letzten Jahre haben gezeigt, dass die Ursachen für Netzausfälle vielfältig sein können. Natürlich gibt es die höhere Gewalt, bei der schon (wie im vor genannten Beispiel) ein umgefallener Baum weitreichende Effekte erzielen kann. Dies gilt erst recht für Naturkatastrophen wie Hochwasser, Waldbrände, extreme Wetterlagen – bis hin zu dramatischen Ereignissen wie ein Tsunami.

Etablierte GSM-Netze erweisen sich hierbei in vielerlei Hinsicht als verwundbar: Sendemasten oder Querleitungen werden zerstört, der Strom fällt aus, die Akkus der Handys können nicht wieder aufgeladen werden. Exakt diese Erfahrung machten die Rettungskräfte beim Elbehochwasser 2002. Die Stromversorgung fiel aus und nach kurzer Zeit konnten die Rettungskräfte nicht mehr per Handy erreicht werden. Damit

eine Grundkommunikation überhaupt möglich war, wurden kurzfristig mehrere Hundert e*Cityruf-Endgeräte von e*Message eingesetzt.

Vor allem aber brechen die Netze, die innerhalb der Zellen eine limitierte Kapazität haben, schon alleine aufgrund der Überlastung ad hoc zusammen. Wenn alle gleichzeitig telefonieren wollen (oder müssen), geht nichts mehr. Diesen Effekt kennt wohl jeder aus persönlicher Erfahrung: Etwa aus der Silvesternacht kurz nach zwölf oder vom Public Viewing der Fußball-WM in Berlin. Was in diesen Fällen meist nur ärgerlich ist und zu Frustrationen Anlass gibt, kann in Katastrophenfällen lebensgefährdende Folgen haben. Um darauf vorbereitet zu sein, wurde beispielsweise in Berlin beim Public Viewing vor dem Brandenburger Tor von den Sicherheitskräften auf den Bündelfunkdienst e*Dispatch gesetzt.

Eine konstante Bedrohung ist durch Attentate wie den zitierten Bombenanschlägen in London gegeben. Als präventive Maßnahme gibt es gezielte Abschaltungen der GSM-Netze etwa bei hochrangigen Staatsbesuchen. Was einerseits Attentate (etwa durch Fernzündungen über Handys wie in Madrid) verhindern soll, schafft andererseits bei einem tatsächlichen Zwischenfall neue Probleme.

Wie simple Stromausfälle zu stundenlangen Zusammenbrüchen von mobilen Telefonnetzen führen können, haben die Nutzer (etwa von D1, E-Plus oder o2) immer wieder erfahren müssen. Ein Risiko, dass sich wohl kaum wird vollends ausschließen lassen.

Als weitere „Störquelle“ gibt es sogenannte GSM-Jammer, kleine Störsender, die in Deutschland zwar illegal sind, aber höchst wirkungsvoll im nächsten Umkreis alle Handy-Verbindungen kappen. Ein Risiko, das mit professionellen Systemen wie dem Funkruf von e*Message vermieden wird.

Blackout im Münsterland

Ein außergewöhnlich heftiger Wintereinbruch hat am ersten Adventwochenende 2005 im nördlichen Münsterland zu chaotischen Verhältnissen geführt. Eisregen und Schneelasten haben nicht nur Stromkabel abgerissen, sondern riesige Masten wie Streichhölzer knicken lassen. In der Folge kam es zu einem tagelangen totalen Stromausfall – und zu massiven Störungen im Bereich der GSM-Netze. Wäre ein solcher „Blackout“ unter normalen Verhältnissen schlimm genug, führt er in Notsituationen zu einem fatalen Teufelskreis: Der Wintereinbruch bringt Menschen in Not (etwa durch im Schnee eingeschlossene Fahrzeuge), gleichzeitig wird eine effektive Hilfe durch eben dieselben Bedingungen erschwert. Genau jetzt müsste die Alarmierung und Koordination von Feuerwehren, Autobahnmeistereien oder Hilfsdiensten perfekt und reibungslos funktionieren – tut es aber nicht.

Die Situation ist vergleichbar mit einem Sicherheitsgurt, der immer funktioniert, nur dann nicht, wenn er gebraucht wird. Kein Mensch würde sich mit einer technischen Lösung einverstanden erklären, die einen Airbag im Falle eines Crashes per Handy-Signal auslöst. Aber offenbar bedarf es Katastrophen wie den Wintereinbruch im Münsterland, um im Nachhinein die Erfahrungen aufzuarbeiten und entsprechende Schlussfolgerungen zu ziehen. Dabei zeigt sich immer wieder, dass die besten Notfallpläne nichts helfen, wenn es mit der Kommunikation nicht klappt. Also müssen professionelle Systeme etabliert und, wo nötig, Redundanzen aufgebaut werden.

Paging ist „krisenresistenter“

Was im großen Maßstab bei Naturkatastrophen gilt, trifft in ähnlicher Weise im betrieblichen Bereich zu. Während man sich im IT-Bereich von Unternehmen oftmals der Risiken bewusst ist und nach sicherheitsrelevanten Lösungen gesucht wird, gerät die mobile Kommunikation allzu häufig aus dem Fokus. Dr. Dietmar Gollnick, Vorsitzender der Geschäftsführung der e*Message Deutschland GmbH: „Während jeder Chef eines Rechenzentrums weiß, dass er getrennte, unabhängige Leitungseinführungen benötigt und dass er für die Datenerhaltung gespiegelte Festplatten braucht, macht er sich über die Abhängigkeit von der herkömmlichen Mobiltelefonie jedoch kaum oder gar keine Gedanken.“

Dabei zeigen die Erfahrungen in Krisensituationen, dass es zwar bequem, aber eben leichtfertig ist, sich ausschließlich auf GSM zu stützen. Im Unterschied zu herkömmlichen Kommunikationsdiensten erweist sich die Paging-Technologie als „krisenresistenter“. Die Technik von e*Message sendet mit 100 Watt im Frequenzbereich um 460 MHz, die ein hohes Durchdringungsvermögen haben und deshalb auch dort Empfang haben, wo Handys versagen (z.B. in der Tiefgarage oder im Aufzug). Vor allem aber ist die Technik so ausgelegt, dass eine Überlastung wie bei GSM ausgeschlossen ist. Wirkungsvoll ist hier auch, dass Sendezellen überlappen und im Ernstfall eine Sendezelle die Aufgabe einer anderen mit übernehmen kann – so passiert, während Kyrill im Ohrekreis wütete. Weshalb dies auch als klarer Vorteil der dortigen Verantwortlichen herausgestellt wurde.

Um Fragen der Sicherheit geht es auch regelmäßig beim jährlich stattfindenden Nationalen Paging-Kongress in Berlin. Hier steht die Alarmierung der Bevölkerung sowie der Hilfs- und Rettungskräfte im Katastrophenfall im Vordergrund. In diesem Zusammenhang wurde vor einem Jahr eine Studie zitiert, die im Auftrag der weltweit führenden Industrievereinigung im Mobiltelefonbereich „Memorandum of Understanding GSM“ (GSM MoU) erstellt wurde. Ihre Schlussfolgerung hat an Aktualität nichts eingebüßt: „Mobiltelefone sind für die Alarmierung und Warnung unmittelbar vor und während der Katastrophe nicht geeignet.“ Hierfür werden Broadcast-Netze, möglichst satellitenbasiert, empfohlen.

Neben dem Argument des Ausfalls der GSM-Netze durch Naturgewalten wurde in der Studie hervorgehoben, dass Broadcast-basierte Dienste wie flächendeckendes Paging „one-to-many“-Technologien sind, also gleichzeitig und schnell möglichst viele Menschen erreichen (und warnen) können. Auch wurde betont, dass Textinformationen in Nottfällen deutliche Vorteile gegenüber Sprachnachrichten haben.

Maßgeschneiderte Services

Von e*Message, dem kontinentaleuropäischen Marktführer in Paging-Dienst und Data Broadcast, gibt es für Kritische Infrastrukturen gleich mehrere professionelle Lösungen und Services. Für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) stellt **e*BOS** eine professionelle Alarmierung sicher. Mit dem klassischen Paging Service **e*Cityruf** können Unternehmen ihre Mitarbeiter schnell und unkompliziert erreichen. Und mit **e*Dispatch** hat e*Message für Unternehmen im

Großraum Berlin-Brandenburg einen leistungsfähigen Bündelfunkdienst für Sprach- und Datenkommunikation etabliert.

Zugeschnitten auf die jeweilige Aufgabenstellung, schaffen alle drei Services die Voraussetzung für eine störungsfreie Informationsübermittlung – auch in Krisensituationen. Und werden sie gar miteinander kombiniert, schaffen sie ein Höchstmaß an professioneller Sicherheit.

e*Message ist in besonderer Weise mit den Herausforderungen der Bundeshauptstadt vertraut. Wie nirgends sonst in Deutschland fokussieren sich Sicherheitsrisiken auf den Ballungsraum. Zur großen Einwohnerzahl einer Metropole (3,4 Mio.) kommen die herausragende Stellung als Regierungssitz, eine hohe Dichte an Botschaften, die Präsenz von internationalen Spitzenorganisationen, symbolträchtige Bauwerke, dichte Verkehrsnetzstrukturen und öffentliche Einrichtungen.

e*BOS: Nicht-öffentliche Alarmierung

Die digitale Alarmierungslösung e*BOS ist exklusiv für Feuerwehren, Rettungsdienste und Hilfsorganisationen konzipiert. Mit ihr können in Deutschland flächendeckend Hilfskräfte zu ihren Einsätzen gerufen werden. Besondere Bedeutung fällt e*BOS vor dem Hintergrund zu, dass bis 2010 in Deutschland ein bundeseinheitliches digitales Sprech- und Datenfunknetz für Behörden und Organisationen mit Sicherheitsaufgaben aufgebaut werden soll, das einer Ergänzung für die Alarmierung bedarf.

Die Beispiele für die erfolgreiche Nutzung der e*BOS-Alarmierung reichen vom hohen Norden bis ins Ruhrgebiet. So werden die Feuerwehren des Kreises Schleswig-Flensburg seit Juli 2006 nicht mehr über ihr veraltetes analoges Funknetz, sondern über die nicht-öffentliche, digitale e*BOS-Alarmierung zu Einsätzen geholt. Bereits nach kurzer Zeit konnten weit über 1.000 Feuerwehrleute über ihre e*Alarm-Meldeempfänger erreicht werden. Kreisbrandmeister Walter Behrens: „Das ist exorbitant! Wir fanden überraschend schnell zu einem reibungslosen Ablauf.“ Auch in Sachsen-Anhalt und Niedersachsen haben sich mit dem Ohrekreis und dem Landkreis Osnabrück die Feuerwehren für die e*BOS-Alarmierung entschieden..

Bei der Entscheidung der Feuerwehren für e*BOS kommen immer wieder dieselben Argumente zum Tragen: e*BOS ist schnell, zuverlässig und kostengünstig, hat eine sehr gute Inhouse-Versorgung und führt zu einer Erreichbarkeit, die weit über die Kreisgrenzen hinausreicht. Die komfortable e*BOS-Meldeempfängerverwaltung, die von e*Message exklusiv für den BOS-Bereich entwickelt wurde (sie ermöglicht nicht nur eine übersichtliche Verwaltung der Meldeempfänger, sondern auch eine einfache Programmierung) gilt als weiteres Plus. Mit der Umstellung der Alarmierung der Werkfeuerwehr der ThyssenKrupp Steel AG auf e*BOS (u.a. in Duisburg, Bochum, Dortmund) ist das Netz auch in Nordrhein-Westfalen verfügbar.

e*Cityruf: schnell und zuverlässig

Der e*Cityruf stellt als klassischer Paging-Dienst seine Leistungsfähigkeit tagtäglich unter Beweis: Hunderttausende von Nutzern, Behörden und namhafte Unternehmen vertrauen auf den klassischen Funkruf-Dienst von e*Message.

Die Vorteile sind evident: Das Funkrufnetz bietet eine hohe Flächenabdeckung, das heißt nahezu alle Funkrufe kommen beim Empfänger an. Hinzu kommt die Erreichbarkeit auch in baulich schwierigen Bereichen (z.B. in Fahrstühlen, Tiefgaragen, Tunneln), wo Mobiltelefone ihren Dienst versagen. e*Cityruf-Empfangsgeräte sind „strahlungspassiv“, weshalb sie u.a. auch in Krankenhäusern, Kraftwerken oder Serverräumen eingesetzt werden dürfen. Mit nur einer einzigen Rufaussendung (Punkt-zu-Multipunkt-Kommunikation) können gleichzeitig Hunderte Empfänger kontaktiert werden – je nach Anwendung auch mehr. Die Nachrichten können einfach und komfortabel über Telefon, Internet, Operatorservice oder E-Mail versendet werden. Da die e*Cityruf-Empfangsgeräte eine Batterielebensdauer von mindestens vier Wochen haben, geht ihnen auch in Notsituationen nicht so schnell der Saft aus. Außerdem sind sie robust und leicht zu bedienen.

Für Firmen mindestens ebenso wichtig sind die Kostenvorteile: Bei e*Cityruf fallen über eine feste monatliche oder jährliche Pauschale hinaus keine nutzungsabhängigen Gebühren an.

Entsprechend der großen Verbreitung von e*Cityruf gibt es die unterschiedlichsten Anwendungsbeispiele, wobei häufig Kritische Infrastrukturen betroffen sind – von medizinischen Einrichtungen bis zu Transport, Logistik und Verkehr. Nicht wegzudenken ist der Paging-Dienst in der Benachrichtigung bzw. Alarmierung von sicherheitsrelevanten Einrichtungen wie Ärzteruf oder Winterdienst, bei automatischen Störmeldungen und in der Anlagenüberwachung.

e*Dispatch: Bündelfunknetz im Großraum Berlin

Der englische Begriff „dispatch“ lässt sich übersetzen mit: abschicken, versenden, prompt und eilig erledigen! All dies sind zutreffende Beschreibungen des neuesten Services von e*Message, nämlich dem e*Dispatch. Dabei handelt es sich um ein Bündelfunknetz zur mobilen Sprach- und Datenkommunikation für geschlossene Benutzergruppen (siehe Kasten: „Bündelfunk“) im Großraum Berlin und in der Region Brandenburg Nord-Ost. Das Netz umfasst rund 30 Funkstandorte, darunter die größte Bündelfunkzelle Europas auf dem Fernsehturm am Berliner Alexanderplatz.

Die besonderen Vorteile des Bündelfunks sind: schneller Rufaufbau (Push-to-Talk / PTT), kurze Rufnummern, logisches Rufnummernkonzept, Sprach-Flatrate innerhalb des Funknetzes, hohe Verfügbarkeit auch bei Massenveranstaltungen, Katastrophen etc., Gruppenruf, schnelle und sichere Datenübertragung und robuste wie langlebige Geräte.

Zu den Nutzern von e*Dispatch gehören die S-Bahn Berlin, die Berliner Stadtreinigung und die Bundespolizei. Per e*Dispatch werden Krankentransporte, Verkehrsampeln sowie Taxis, Sicherheits- und Kurierdienste gesteuert.

Bei vielen Praxisbeispielen handelt es sich um Kritische Infrastrukturen. Ergo sind die hohe Zuverlässigkeit und Leistungsfähigkeit des Bündelfunknetzes bei gleichzeitig sehr guter Flächenabdeckung in der Hauptstadtregion, wo spezielle Sicherheitsanforderungen an öffentliche wie private Unternehmen gestellt werden, von besonderer Bedeutung.

Sich gegen kommunikativen Blackout wappnen

e*BOS, e*Cityruf und e*Dispatch - mit den verschiedenen Diensten von e*Message wird das ganze Spektrum sicherheitsrelevanter, mobiler Kommunikation abgedeckt. Angefangen von Transport und Verkehr über Energie- und Finanzwesen bis hin zu polizeilichen Einrichtungen und Rettungswesen.

Für Unternehmen aller Branchen bietet sich die Chance, sich gegen kommunikativen „Blackout“ zu wappnen. Voraussetzung ist, dass die Gefahren und die Folgen einer solchen Störung überhaupt erkannt werden. Von Expertenseite wird deshalb dringend angeraten, ein Worst-case-Szenario durchzuspielen und die Risiken sowie ihre wirtschaftlichen Konsequenzen zu analysieren. e*Message bietet hier präventive Gefährdungs-Analysen an. Auf Basis der Ergebnisse lässt sich dann sehr schnell abschätzen, ob sich die Investition in eine verbesserte mobile Kommunikation lohnt. Wobei auch hier gilt, was sich am Steuer eines Automobils zeigt: Kein vernünftig denkender Mensch verzichtet auf Sicherheitsgurt und Airbag. Das Risikobewusstsein ist durch persönliche Erlebnisse und Beobachtungen im Straßenverkehr sowie durch die Medienberichterstattung so weit entwickelt, dass dies grob fahrlässig erschiene. Im professionellen Bereich der mobilen Kommunikation herrscht dagegen häufig noch eine unbekümmerte Zuversicht vor, die sich alleine dadurch erklärt, dass die Gefahren eines Crashes nur selten drastisch vor Augen geführt werden und sich deshalb leichter verdrängen lassen.

Mit wenigen, einfachen, Fragen lässt sich rasch feststellen, ob die gefühlte Sicherheit trügerisch ist:

- Kann ich bzw. mein Unternehmen / meine Behörde noch kommunizieren, wenn die mobilen Kommunikationssysteme ausgefallen sind?
- Wenn nicht, welche Konsequenzen entstehen daraus?
- Wie ist der ökonomische Schaden einzuschätzen?
- Muss ich mich gegen diesen „worst case“ absichern?

KASTEN (1)

Bündelfunk

Beim Bündelfunk, wie ihn e*Dispatch im Großraum Berlin und in der Region Brandenburg Nord-Ost anbietet, handelt es sich um ein leistungsfähiges und sicheres Funknetz für geschlossene Benutzergruppen. Es ist maßgeschneidert für die zentrale Steuerung von Mitarbeitern, die sich in definierten Räumen bewegen. Die Informationsübermittlung kann per digitalen (*wirklich digital?*) Datenaustausch erfolgen und/oder über (kurze) analoge Gespräche. Technisch liegt dem Bündelfunk ein „Bündel“ an Frequenzen (410 bis 430 MHz) zugrunde, die über einen digitalen Organisationskanal den Teilnehmern für die Dauer der Informationsvermittlung zugeteilt werden. Die Übertragung kann im Einzelruf erfolgen oder als Gruppenruf,

mit dem sich alle oder ein ausgewählter Teil der Mitarbeiter erreichen lassen. Darüber hinaus ermöglicht e*Dispatch den Übergang aus dem Bündelfunk ins öffentliche Telefonnetz (im Wechselsprechverfahren). Da der Bündelfunk ausschließlich mit limitierten Teilnehmergruppen arbeitet, kann eine unkontrollierte Überlastung (etwa bei Massenveranstaltungen) ausgeschlossen werden. Hinzu kommt: Die größte Funkzelle Europas auf dem Fernsehturm am Alexanderplatz bleibt auch bei einem großflächigen Stromausfall über eine Notversorgung funktionsfähig.

Die Vorteile - wie schneller Rufaufbau (Push-to-Talk) und sichere Informationsübertragung - machen e*Dispatch zu einem idealen Medium nicht nur für Taxiunternehmen oder Kurierdienste, sondern insbesondere auch für Organisationen mit sicherheitsrelevanten Aufgaben (z.B. Rettungsdienste). Wobei je nach Grad des Anforderungsprofils der Bündelfunk als ausschließliches Funknetz oder als Backup für Notsituationen eingesetzt werden kann.

KASTEN (2)

Im Ernstfall ungeeignet

Häufig genutzte mobile Kommunikationsdienste erweisen sich im Ernstfall als ausgesprochen störanfällig. Im folgenden einige Beispiele:

Tsunami in Südostasien: Die von einem Seebeben im Indischen Ozean ausgelöste Flutwelle führte am 26. Dezember 2004 zu einem weitgehenden Zusammenbruch der betroffenen Mobiltelefonnetze.

Hurrikan Katrina: Als im August 2005 ein tropischer Wirbelsturm vor allem im Großraum New Orleans verheerende Auswirkungen hatte, erwies sich Paging als wesentlich stabiler als Mobiltelefon-Technologien. Es gab kaum längere Ausfälle.

Schneekatastrophe im Münsterland: Ein außergewöhnlich heftiger Wintereinbruch hat am ersten Adventswochenende 2005 im nördlichen Münsterland Strommasten geknickt, Stromkabel abgerissen, das GSM-Netz lahm gelegt. Die Folge war ein totaler Blackout.

Orkan Kyrill: Den Orkan Kyrill vom 18. Januar 2007 haben die Netze der großen Mobiltelefonbetreiber zwar ohne größere Schäden überstanden, aber es kam zu Kapazitätsengpässen bzw. Netzüberlastungen u.a. an Bahnhöfen und Flughäfen. Und in kleineren Regionen zeigte sich exemplarisch die Anfälligkeit der Kommunikationssysteme. Als im Ohrekreis (Sachsen-Anhalt) der Strom, teilweise auch Telefon- und Handynetze sowie die Sirenen ausfielen, außerdem ein Blitz in einen Sendemast einschlug, bewährte sich die digitale Alarmierung e*BOS. Sie ermöglichte eine zuverlässige und rasche Koordinierung der Feuerwehr-Einsatzkräfte.

Bombenanschläge am 7. Juli 2005 in London: Hauptursache für die erheblichen Schwierigkeiten bei der Rettung von Verletzten war der Zusammenbruch der örtlichen Telefon- und Mobiltelefonnetze. In der Konsequenz hat der London Ambulance Services ein Pager-System in die Alarmkette integriert.

Flächendeckender Stromausfall in Westeuropa: Am 4. November 2006 kam es nicht nur zu einem Zusammenbruch des Energie-Verbundnetzes (der bis nach Nordafrika reichte), sondern in der Folge auch zu einem Ausfall der Festnetz- und Mobiltelefonnetze. Dagegen arbeiteten die Paging-Services von e*Message völlig störungsfrei.

Explosionskatastrophe im niederländischen Enschede: Am 13. Mai 2000 ging eine Feuerwerksfabrik in Flammen auf. Ein ganzer Ortsteil fühlte sich aufgrund der Explosionen wie im Krieg. Eine Warnung über Mobiltelefonnetze scheiterte am Zusammenbruch des Systems.

Jahrhunderthochwasser an der Elbe: Im Jahr 2002 verloren nicht nur Zehntausende Bewohner ihr Hab und Gut in den Wassermassen, auch erwies sich die Koordination der Rettungskräfte, Soldaten und Fluthelfer als äußerst schwierig. In dieser Situation funktionierten nur noch die Paging-Services.

Terroranschläge vom 11. September in den USA: Sowohl in New York als auch beim Pentagon in Arlington (Virginia) und in Pittsburgh (Pennsylvania) kam es mit den Terroranschlägen zu folgenschweren Ausfällen der Mobiltelefonnetze.

Waldbrände in Südeuropa: Im trockenen Sommer 2003 führten ausgedehnte Waldbrände u.a. in Portugal und Südfrankreich zu Schwierigkeiten bei der Warnung der Bevölkerung, weil die Mobiltelefonnetze außer Betrieb gingen.

Regionale Ausfälle in Deutschland: Überlastungen bei der Fußball-WM oder in der Silvesternacht, durchtrennte Glasfaserkabel, Stromausfälle oder Fehler in Vermittlungsstellen – immer wieder kommt es in Deutschland zu Störungen und Ausfällen in den Mobiltelefonnetzen der verschiedenen Netzbetreiber.

GSM-Jammer: Zunehmend werden Fälle bekannt, in denen „Jammer“ zum Einsatz kommen, die das absichtliche Stören von GSM-Verbindungen ermöglichen.