Alcatel-Lucent Stiftung für Kommunikationsforschung

Neue Krisen
Ein Blick in die Zukunft

Albrecht Broemme, Gerd Gräff, Franz-Reinhard Habbel, Reinhold Harnisch, Cornelia Rogall-Grothe, Erich Zielinski

DStGB
Deutscher Städte- und Gemeindebund
www.dstgb.de

105

Neue Krisen
Ein Blick in die Zukunft

Dokumentation der 13. Fachkonferenz „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden“

17. Juni 2013, Berlin

Impressum

Stiftungsreihe 105

Redaktion
Dr. Erich Zielinski
Petra Bonnet M.A.

Druck der Broschüre
DCC Kästl GmbH & Co. KG

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine nichtrechtsfähige Stiftung in der treuhänderischen Verwaltung des Stifterverbandes für die Deutsche Wissenschaft.

Angaben nach § 5 TMD/
§ 55 RfStv

Stifterverband für die Deutsche Wissenschaft e.V.
Barkhovenallee 1
45239 Essen
Telefon: (02 01) 8401-0
Telefax: (02 01) 8401-301
E-Mail: mail@stifterverband.de

Geschäftsführer:
Prof. Dr. Andreas Schlüter
(Generalsekretär)

ISSN 0932-156x

Inhalt

Grußworte

Franz-Reinhard Habbel

Das Thema Sicherheit hat in den letzten Tagen eine besondere Dramatik bekommen: Jeder von uns hat die Bilder der Flut vor Augen mit der Zerstörung von Hab und Gut und vieler Infrastrukturen. Wir haben die Bilder von der beispiellosen Hilfe durch die Bürgerinnen und Bürger im Kopf. Es zeigt sich, dass die Behörden, die Hilfseinrichtungen wie die Feuerwehren oder das Technische Hilfswerk gemeinsam mit Bürgerinnen und Bürger gut zusammenarbeiten. Das läuft alles sehr professionell ab.

Wir danken allen Helferinnen und Helfer, die sich in den vergangen Tagen für das Gemeinwohl eingesetzt und Solidarität gezeigt haben.

Vergleicht man die heutige Flut mit der vor gut zehn Jahren, so zeigt sich, dass sich die Kommunikation verändert hat. Damals stand die Behördenkommunikation z.B. wegen dem fehlenden Digitalfunk in der Kritik. Heute zeigt sich eine breite Helferkommunikation auf der Basis der Selbstorganisation. Sehr viele Menschen organisieren sich über soziale Netzwerke wie Facebook und Twitter. Diese steckten damals noch in den Kinderschuhen – zudem hatte kaum einer eine Digitalkamera geschweige denn ein Handy mit Fotofunktion. Hunderte von Gruppen zur Flut wurden in diesem Jahr in Facebook gegründet. Die Gruppe „Fluthilfe Dresden“ wurde von einem Studenten am ersten Sonntag nach der Flut eingerichtet – 48.000 Follower in 24 Stunden!

Nach den ersten Hilfsmaßnahmen geht es jetzt darum, die Infrastruktur wieder aufzubauen. Bund und Länder wollen insgesamt 8 Mrd. Euro an Hilfen zur Verfügung stellen.

Der Deutsche Städte- und Gemeindebund fordert ein „Hochwasserschutz-Beschleunigungsgesetz“. Überlange Planungsverfahren sollten gekürzt werden, Gemeinnutz vor Eigennutz gestellt werden.

Neben der Organisation und Durchführung der Hilfsmaßnahmen sind Staat und Kommunen, aber auch Wirtschaft und Zivilgesellschaft gefordert, über Konsequenzen nachzudenken, ihre Politik zu überprüfen und wenn notwendig, neu auszurichten. Die Städte und Gemeinden rundum einzumauern, kann nicht die alleinige Lösung sein. Was können wir neben einer schnellen Hilfeleistung tun? Wäre es nicht an der Zeit, ein urbanes Infrastruktur-Management aufzubauen und zu nutzen?

Wir müssen neue Wege gehen. Die erste und wichtigste Erkenntnis ist: Wir können uns nicht gegen alles schützen und versichern! Wir werden mit solchen Naturereignissen leben müssen. Sie sind Folgen globaler und langfristiger Veränderungen der Umwelt, unseres Klimas aber auch der Entwicklung der Menschheit. Das ist die Realität.

Wir müssen akzeptieren, dass notwendige Veränderungen unseres Verhaltens erst Jahrzehnte später wirken werden. Was wir jetzt machen müssen, ist die Widerstandsfähigkeit der Städte und Gemeinden zu erhöhen. Die Aufgabe lautet: Schaffen wir resiliente Städte!

Unter Resilienz verstehen wir die Widerstandsfähigkeit einer Gesellschaft, ihre Fähigkeit, eine plötzliche Katastrophe oder eine Krise rasch zu bewältigen und die Funktions- und Handlungsfähigkeit schnellstmöglich

wieder herzustellen. Eine umfassende Gewährleistung von Sicherheit ist angesichts der Vielfalt, der Komplexität und der Unvorhersehbarkeit moderner Risiken nicht mehr möglich. Durch Resilienz soll die Widerstands- und Regenerationsfähigkeit von technischen und gesellschaftlichen Systemen erhöht werden. Resilienz ist wie eine Feder. So lange sie elastisch ist, springt sie immer wieder in den ursprünglichen Zustand zurück. Das gilt auch für Kommunen.

Das heißt, wir brauchen eine Flexibilität und vor allen Dingen ein ganzheitliches Vorgehen. Notwendig ist ein Systemdenken. Ein solches Denken ist in den Städten aber nur bedingt vorhanden. Rechenzentren könnten hier Impulse geben.

Die Sicherheit in unseren Städten ist aber nicht nur durch Naturkatastrophen bedroht. Die Einbrüche haben in Deutschland rasant zugenommen, alle vier Minuten wird in Deutschland eingebrochen. Die Aufklärungsquote liegt bei diesen Delikten bei 15 Prozent.

Im ländlichen Raum hat sich die Polizeipräsenz verschlechtert - oft brauchen Polizisten zum Tatort mehr als eine halbe Stunde Anfahrt. In Nettersheim wurde überlegt, eine Art Bürgerwehr einzurichten.

Bedrohliche Ausmaße hat auch das Thema Cybersicherheit angenommen. Cyber-War ist keine Spielveranstaltung von Freaks, sondern inzwischen Realität. Im Sekundentakt werden Netze verseucht und Server angegriffen. Die IT-Sicherheit wird eine ganz zentrale Aufgabe. Die Wehretats in den Industriestaaten werden umgeschichtet. Die Ausgaben für Abwehrtechnik im IT-Bereich werden immens steigen.

Der Verfassungsschutzpräsident Maaßen hat zu einer strategischen Allianz zum Schutz der eigenen Wirtschaft aufgerufen. Die IT-Sicherheitsexpertin Natalja Kasperskaja hat in einem bemerkenswerten Interview der WELT darauf hingewiesen, dass die Zahl der Datendiebstähle jährlich um 30 bis 50 Prozent wächst. Sie sehe nicht, wie dieser Trend in nächster Zeit gestoppt werden könnte.

Die Kritischen Infrastrukturen nehmen in Wirtschaft, Verwaltung und Gesellschaft inzwischen eine besondere Rolle ein. Die meisten Systeme, von der Energie- oder Wasserversorgung über Gesundheit bis hin zu Bankautomationen sind von IT und im wesentlichen vom Strom abhängig. Auch hier kommt dem Thema Sicherheit eine immer wichtigere Rolle zu.

Franz-Reinhard Habbel
Sprecher des Deutschen Städte- und Gemeindebundes, Berlin

Grußworte

Erich Zielinski

Ich begrüße Sie auf das Herzlichste bei der diesjährigen Veranstaltung der Alcatel-Lucent Stiftung und des Deutschen Städte- und Gemeindebundes zur Sicherheitskommunikation.

Mein besonderer Dank geht auch in diesem Jahr an die Landesvertretung Baden-Württemberg, in welcher wir immer mit großer Gastfreundschaft empfangen werden und die einen atmosphärisch herrlichen Rahmen bietet.

Das Thema Sicherheitskommunikation hat mittlerweile eine langjährige Tradition bei der Stiftung. Das beteiligte Netzwerk der Stiftung verfolgt dabei das Ziel, die Erörterungen in diesem Themenfeld inhaltlich-konzeptionell voranzutreiben, neue Entwicklungen und Ideen vorzustellen und vor allem den Erfahrungsaustausch zwischen Wissenschaft und Praxis zu fördern.

Die diesjährige Veranstaltung steht unter dem Motto „Neue Krisen: Ein Blick in die Zukunft“. Die Konferenz wird eröffnet mit einem Vortrag über die „Nationale Allianz für Cybersicherheit“. Frau Rogall-Grothe, Staatssekretärin im Bundesministerium des Innern und zugleich Vorsitzende des Cyber-Sicherheitsrates, wird hierzu Strategien vorstellen.

Über die fatalen Folgen, die Extremwetterereignisse für die Sicherheit haben können, und die dazu gegründete Behördenallianz wird Christoph Unger, Präsident des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, informieren. Das Thema hat einen aktuellen Bezug erhalten, der bei der Konzeption der Konferenz natürlich so nicht zu erahnen war.

Am Vormittag steht ein Blick in die Zukunft auf dem Programm. Es werden die Bereiche Forschung für die Sicherheit vorgestellt, Drohnen in der zivilen Nutzung sowie der Ausfall von Internet- und Mobilfunknetzen thematisiert.

Der Nachmittag steht ganz im Zeichen der praktischen Erörterung von Fragen zur Vorbereitung von Kommunen auf den Notfall.

- Wie können kritische Infrastrukturen im Notfall geschützt und die IT-Systeme krisenfest gemacht werden?
- Wie kann sich eine Gemeinde auf einen Katastrophenfall vorbereiten?
- Wie kommuniziert man in der Krise?

Diese und weitere Fragen werden Andreas Memmert, Bürgermeister der Stadt Schladen, Reinhold Harnisch, Kommunales Rechenzentrum Minden-Ravensburg / Lippe, der Präsident des Technischen Hilfswerkes, Albrecht Broemme, und Rolf Krost, Präsident der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, beantworten.

Im abschließenden Vortrag wird Gerd Gräff, Abteilungsleiter für Katastrophenschutz und Krisenmanagement im Ministerium des Innern, für Sport und Infrastruktur Reinland-Pfalz, über die strategische Ausrichtung der neu eingerichteten zentralen Koordinierungsstelle zum Schutz kritischer Infrastrukturen informieren.

In einem anschließenden Expertengespräch werden die Fragen noch einmal aufgegriffen und vertieft.

Aus den Diskussionen und dem Austausch unterschiedlichster Institutionen und Akteure entwickelte sich zugleich das Verständnis über Sicherheitskommunikation weiter: Es muss auch die Organisation und die soziale Komponente der Kommunikation stimmen, denn im Katastrophenfall müssen alle zu optimierenden Aspekte auch tatsächlich optimal miteinander funktionieren.

Die Stiftung ist im Laufe der Zeit und ihrer Beschäftigung mit der Thematik an derselben gewachsen und bietet zwischenzeitlich eine neutrale und anerkannte Plattform, auf welcher weiterentwickelt und gemeinsam gestaltet werden kann.

Meine Damen und Herren, ich bin mir sicher, dass diese Konferenz auch heute wiederum eine überaus gute Gelegenheit bieten wird, von renommierten Experten Neues zu erfahren und darüber zu diskutieren.

Genauso wichtig wie der zu erwartende hochwertige Input ist für mich immer die Chance zur Diskussion, zum Austausch und zur Intensivierung der Kontakte untereinander und zwischen den einzelnen Institutionen, die sich der Sicherheitskommunikation und dem Schutz kritischer Infrastrukturen verschrieben haben.

Lassen Sie uns diese Chance nutzen!

Ich wünsche uns allen einen interessanten und ertragreichen Verlauf der Fachkonferenz

Dr. Erich Zielinski
Direktor der Alcatel-Lucent Stiftung

Nationale Allianz für Cyber-Sicherheit

Cornelia Rogall-Grothe

Ich möchte mich zunächst bei den Initiatoren dieser Fachkonferenz für die Gelegenheit bedanken, über das uns zurzeit alle bewegende Thema Cyber-Sicherheit sprechen zu können.

Bevor ich hierzu und zu anderen Bedrohungen nähere Ausführungen machen werde, möchte ich Ihnen die Relevanz des Internet für unsere Gesellschaft und für das Wohlergehen Deutschlands verdeutlichen.

- Etwa 80 % aller Deutschen nutzen das Internet[1] – für geschäftliche als auch für private Aktivitäten.
- Ca. 74 % der Internetnutzer sind in mindestens einem sozialen Netzwerk angemeldet.
- 97 % der Klein- und Mittelständischen Unternehmen nutzen E-Mails und 98 % nutzen das Internet für geschäftliche Zwecke.
- Note- und Netbooks, Smartphones und GPS-Navigation sind aus unserem Alltag nicht mehr wegzudenken.
- Im täglichen Gebrauch des Internet haben Bürgerinnen und Bürger kennen und schätzen gelernt, Vorgänge des täglichen Lebens vollständig und einfach online abwickeln zu können. Die gleiche Einfachheit und Durchgängigkeit erwarten sie dann auch, wenn sie mit Behörden in Kontakt treten. Aus diesem Grunde bieten immer mehr Städte und Gemeinden im Rahmen ihrer e-Government-Strategie Dienstleistungen für Bürgerinnen und Bürger sowie für die Wirtschaft über das Internet an. Die Angebote reichen von umfangreichen Städteportalen über die Online-Terminvereinbarungen beim Amt bis hin zu komplexen Beteiligungsverfahren bei der Bauleitplanung.

Zusammenfassend bietet das Internet

- für Unternehmen die Chance, wirtschaftlich erfolgreich zu sein und ihre Prosperität zu stärken;
- für Verwaltungen die Möglichkeit, Dienstleistungen effektiver und effizienter und damit kostengünstiger anzubieten.

Dies ist die Sonnenseite des Internet.

Aber leider gibt es auch eine Schattenseite. Diese Schattenseite ist geprägt durch Computerkriminalität, Computersabotage und Computerspionage.

- Seit 2005 werden zielgerichtete Angriffe auf Bundesbehörden und Industrie mittels Spionage-Trojaner beobachtet.
- Bot-Netze erlauben eine Fernsteuerung von Millionen zuvor mit Schadsoftware infizierter Systeme. So wurden bereits 2007 Server der estnischen Regierung, von Banken, Zeitungen und vereinzelten Unternehmen Ziel konzertierter DDoS-Angriffe auf der Basis eines Botnetzes. Estland war massiv gelähmt und benötigte technisch wie organisatorisch zwei Wochen, um die Angriffe abzuwehren. Ähnlich erfolgten Angriffe auf Malta (2004) und Georgien (2008).
- Das Internet ist auch Ort krimineller Aktivitäten. Die Angreifer müssen keine IT-Experten mehr sein. Sie können Schwach-

1 Quelle: DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet, Sinus-Institut, Hamburg 2012

stellen und Dienstleistungen (bis hin zur kompletten Durchführung von Angriffen) im Internet einkaufen.

- Die Anzahl der begangenen Straftaten und die Schadenshöhen steigen in Deutschland stetig an. Von 2006 bis 2011 hat sich die in der polizeilichen Kriminalstatistik erfasste IuK-Kriminalität von ca. 30.000 auf ca. 60.000 Fälle verdoppelt. Die Höhe der registrierten Schäden ist im selben Zeitraum um 70 % gestiegen.
- Mitte Mai gelang Kriminellen der Diebstahl von 45 Mio. US-Dollar durch manipulierte ausländische Bankkarten dadurch, dass Hacker Sicherheitsprotokolle einer Bank knackten, das Limit für Abhebungen aufhoben und die Informationen weltweit an Komplizen verteilten. Die Abhebungen der 45 Mio. US-Dollar von den geknackten Konten fanden im Dezember 2012 und im Februar 2013 binnen weniger Stunden statt. Bankkarten deutscher Banken waren nicht betroffen, das Verfahren ist hier auch technisch gar nicht möglich. Dieses Beispiel zeigt aber, dass es unabdingbar ist, die Erhöhung der Cyber-Sicherheit international zu koordinieren.
- Es vergeht heute fast kein Tag mehr, ohne dass ein neuer Cyber-Angriff bekannt würde. Derzeit werden täglich durchschnittlich 13 neue Schwachstellen in Standardprogrammen entdeckt und weltweit ca. 21.000 Webseiten mit Schadprogrammen infiziert. Durchschnittlich alle zwei Sekunden wird ein neues Schadprogramm beziehungsweise eine Variante eines Schadprogrammes erstellt.

Stuxnet hat uns 2010 erstmals vor Augen geführt, dass die Aufklärung, insbesondere durch Sammlung von Informationen zur Abschätzung der Bedrohung einschließlich der zu erwartenden Folgen, eine erhebliche Zeit in Anspruch nehmen kann. Die seit 2011 erfolgten Angriffe auf Sicherheitsarchitekturen des Internet oder Sicherheitsunternehmen selbst tangieren sogar die Grundfesten der bisherigen weltweiten Sicherheitsmaßnahmen.

Die aufgeführten Beispiele zeigen in eindringlicher Weise, dass Gegenmaßnahmen ergriffen werden müssen, um die Infrastruktur Internet und digitale Netze inklusive der Systeme der Internetnutzer vor solchen Angriffen zu schützen, beziehungsweise die negativen Auswirkungen solcher Angriffe zu minimieren.

Die Bundesregierung hat daher im Februar 2011 die „Cyber-Sicherheitsstrategie für Deutschland“ verabschiedet.

Kernpunkte dieser Strategie sind

- der verstärkte Schutz Kritischer Infrastrukturen vor IT-Angriffen;
- der Schutz der IT-Systeme in Deutschland einschließlich einer Sensibilisierung der Bürgerinnen und Bürger;
- der Aufbau eines Nationalen Cyber-Abwehrzentrums sowie die Einrichtung eines Nationalen Cyber-Sicherheitsrates.

Die Einrichtung eines Nationalen Cyber-Abwehrzentrums war dringend geboten, um die Handlungsfähigkeit bei IT-Vorfällen zu verbessern. Cyber-Kriminelle orientieren sich nicht an Behördenstrukturen oder Zuständigkeiten, so dass eine behördenübergreifende Informationsplattform geschaffen werden musste.

Mit dem Nationalen Cyber-Abwehrzentrum ist es uns gelungen, eine zentrale Informationsplattform auf Bundesebene zu bilden. Sie ermöglicht es, schnell und abgestimmt alle re-

levanten Informationen zu einem IT-Vorfall zusammenzutragen und zu bewerten. Wichtig ist es, insbesondere Empfehlungen zum Schutz der IT-Systeme wie auch Informationen zu weiteren Schadensminimierungsmaßnahmen zur Verfügung zu stellen.

Die im Cyber-Abwehrzentrum vertretenen Behörden haben die unterschiedlichsten Aufgaben, aber ein Ziel gemeinsam: Sie bündeln ihre Erkenntnisse und Erfahrungen hinsichtlich neuer technischer Bedrohungen, die sie im Rahmen ihrer Aufgaben erlangen.

Seit seiner Gründung am 1. April 2011 hat das Nationale Cyber-Abwehrzentrum etwa 900 nationale und internationale IT-Sicherheitsvorfälle vertieft bearbeitet. Im Herbst 2011 nahm es an der Übung LÜKEX 2011 teil, der ersten bundesweiten IT-Sicherheitsübung unter Einbeziehung mehrerer Länder und KRITIS-Betreiber. Nicht zuletzt die Teilnahme einiger Länder an dieser Übung hat bewirkt, dass nunmehr in den Ländern mit dem Aufbau von CERT-Infrastrukturen begonnen wird. Alle Länder erbringen bereits Basisdienste auf den wesentlichen Handlungsfeldern (Vorfallbearbeitung, Warnungen, Information). Zur Integration der Kommunen in die Warn- und Alarmierungsdienste einzelner Länder sind erste Maßnahmen geplant bzw. befinden sich in der Umsetzung. Dies sind sehr positive Ansätze, und ich bitte Sie, sich weiterhin für die Cyber-Sicherheit ihres Landes oder ihrer Kommune zu engagieren.

Der wesentliche Kernpunkt der Cyber-Sicherheitsstrategie betrifft den Schutz der Kritischen Infrastrukturen.

Zum Schutz der Kritischen Infrastrukturen wurde seit 2005 der Umsetzungsplan KRITIS erarbeitet und 2007 beschlossen. Dieser sieht vor, dass Unternehmen Kritischer Infrastrukturen und der Staat eng beim IT-Schutz dieser Infrastrukturen zusammenarbeiten. Dieser kooperative Gedanke hat sich grundsätzlich bewährt und wird mit der Cyber-Sicherheitsstrategie weiterentwickelt.

In die Überlegungen zum Schutz kritischer Infrastrukturen sind alle Betreiber dieser Infrastrukturen einzubeziehen, unabhängig von den Eigentumsverhältnissen oder ihrer Rechtsform, also auch solche KRITIS-Betreiber, die von Kommunen mittelbar oder unmittelbar betrieben werden. Mir wurde berichtet, dass besonders häufig kommunale Unternehmen in den Bereichen Energie und Wasser anzutreffen seien. Die IT-Sicherheit kritischer Infrastrukturen hat im Bundesministerium des Innern höchste Priorität. Um den IT-Schutz Kritischer Infrastrukturen weiter zu stärken, hat Herr Bundesminister Dr. Friedrich im Sommer 2012 Gespräche mit der Leitungsebene verschiedener Betreiber Kritischer Infrastrukturen geführt. Es ist wichtig, dass sich alle Branchen umfassend um die Sicherheit ihrer von IT-abhängigen kritischen Geschäftsprozesse bemühen. Wir brauchen bundesweit einheitliche Mindeststandards und zuverlässige Meldewege, um bei IT-Vorfällen eine schnelle Information und Reaktion aller Betroffenen sicherzustellen. Alle Betreiber Kritischer Infrastrukturen mit Sitz in Deutschland, die zuständigen Aufsichtsbehörden sowie die zugehörigen Fach- und Branchenverbände können Teilnehmer des UP-KRITIS werden. Ich möchte alle ermuntern, sich zu beteiligen. Der Umsetzungsplan KRITIS (UP-KRITIS) hat hierzu Branchenarbeitskreise zum brancheninternen Erfahrungsaustausch neu eingerichtet. Ich fordere Sie hiermit ausdrücklich auf, dem Umsetzungsplan KRITIS beizutreten und gemeinsam an einer Verbesserung der Sicherheit der IT der Kritischen Infrastrukturen mitzuwirken; hierzu wenden Sie sich bitte an das BSI,

das Bundesamt für Sicherheit in der Informationstechnik.

Die von Herrn Bundesminister Dr. Friedrich geführten Gespräche haben gezeigt, dass das Schutzniveau in den einzelnen Branchen trotz der Arbeit im Rahmen des Umsetzungsplans KRITIS immer noch sehr unterschiedlich ist und große Lücken insbesondere in den bisher nicht regulierten Branchen bestehen. Wir brauchen daher einen gesetzlichen Rahmen für mehr Kooperation und die Einhaltung von IT-Sicherheitsstandards. Allein mit freiwilligen Maßnahmen sind wir in der Vergangenheit hinter unseren Zielen zurückgeblieben. Insbesondere haben diese Maßnahmen nicht dazu geführt, dass Unternehmen erhebliche IT-Sicherheitsvorfälle melden und damit dazu beitragen, ein valides nationales IT-Sicherheitslagebild zu erstellen.

Aus diesem Grunde haben wir uns entschlossen, den Entwurf eines IT-Sicherheitsgesetzes vorzustellen. Der Vorschlag enthält im Wesentlichen drei Schwerpunkte:

1. Betreiber Kritischer Infrastrukturen, die von besonderer Bedeutung sind, werden zu einer Verbesserung des Schutzes der von ihnen eingesetzten Informationstechnik und zur Verbesserung ihrer Kommunikation mit dem Staat bei IT-Vorfällen verpflichtet;
2. die Telekommunikations- und Telemediendiensteanbieter werden stärker als bisher für die Sicherheit im Cyber-Raum in die Verantwortung genommen und
3. das Bundesamt für Sicherheit in der Informationstechnik wird in seinen Aufgaben und Kompetenzen gestärkt.

Das Maß der Selbstregulierung sollte hierbei so hoch wie möglich sein und die gesetzlichen Vorgaben im Ergebnis immer auch dazu dienen, für alle Beteiligten einen Mehrwert zu generieren.

Dieser Mehrwert soll für die Unternehmen der Branchen der Kritischen Infrastrukturen darin bestehen, dass das Angebot zur Beratung und Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik ausgeweitet werden soll. Somit haben sowohl der Staat, in Form eines vollständigeren Lagebildes, als auch die Unternehmen einen Mehrwert durch diese Gesetzesinitiative. Hierbei möchte ich insbesondere auch die kommunalwirtschaftlichen Unternehmen als Betreiber Kritischer Infrastrukturen explizit einbeziehen.

Die zunehmende Durchdringung der IT hat dazu geführt, dass auch in anderen Bereichen der Wirtschaft, die bisher noch nicht in den Informationsaustausch mit dem BSI einbezogen waren, Hilfe angeboten werden soll. Das BSI ergänzt in einer mit dem BITKOM gegründeten „Allianz für Cyber-Sicherheit“ den kooperativen Ansatz für nicht-kritische Infrastrukturen. Denn wir müssen auch eine engere Vernetzung mit der Wirtschaft über den KRITIS-Bereich hinaus herstellen, um auch in diesem Bereich IT-Vorfällen zu begegnen, insbesondere zur Abwehr von Sabotage, Spionage, Erpressung und anderer Formen der Cyber-Kriminalität.

Die Allianz für Cyber-Sicherheit bietet allen wichtigen Akteuren aus diesem Bereich in Deutschland eine Plattform. Allgemeine und offene Informationen, die im Nationalen Cyber-Abwehrzentrum und im Umsetzungsplan KRITIS gewonnen werden, werden über diese Plattform auch den an der Allianz für Cyber-Sicherheit beteiligten Institutionen zur Verfügung gestellt. Das BSI, das sowohl im Umsetzungsplan KRITIS als auch im Cyber-Abwehrzentrum sowie in der Allianz für Cy-

ber-Sicherheit beteiligt ist, kann damit sicherstellen, dass für die Cyber-Sicherheit relevante Informationen aufbereitet und allen Beteiligten zur Verfügung gestellt werden.

Die Allianz für Cyber-Sicherheit richtet sich zwar in erster Linie an Unternehmen, aber eine Beteiligung von Universitäten oder anderen Institutionen wie Verwaltungen ist nicht ausgeschlossen. Die Allianz für Cyber-Sicherheit unterscheidet drei Formen der Teilhabe:

1. Teilnehmer: Teilnehmer können alle Institutionen in Deutschland werden, dies schließt sowohl Behörden als auch Universitäten mit ein. Teilnehmer profitieren von den Informationen und Erfahrungsaustauschen der Allianz.
2. Partner: Partner sind Experten für das Thema „Cyber-Sicherheit“. Partner bringen sich mit ihrem Know-how in die Allianz ein und fördern somit die Cyber-Sicherheit in Deutschland aktiv.
3. Multiplikatoren: Multiplikatoren sind Verbände, Gremien oder Medien, die die Wirkung der Allianz in die Fläche bringen wollen.

Bislang engagieren sich über 290 Institutionen in der Allianz für Cyber-Sicherheit, davon über 205 Institutionen aus Wirtschaft und öffentlicher Verwaltung als Teilnehmer, über 65 Institutionen als Partner sowie BITKOM und einige andere Institutionen als Multiplikatoren.

Um das bereits durch Meldungen im Umsetzungsplan KRITIS und im Cyber-Abwehrzentrum erstellte Lagebild zu ergänzen, wurde eine zentrale Meldestelle für anonymisierte Meldung von IT-Angriffen eingerichtet.

Die Instrumente der Allianz für Cyber-Sicherheit sind das Informationsangebot und der Erfahrungsaustausch. Das Informationsangebot zum Thema Cyber-Sicherheit wächst kontinuierlich. Die Mehrzahl der Informationen wird öffentlich auf den Webseiten der Allianz für Cyber-Sicherheit veröffentlicht. Zum Erfahrungsaustausch zwischen den Institutionen veranstaltet die Allianz für Cyber-Sicherheit regelmäßige Treffen sowohl für Partner als auch für Teilnehmer.

Meine sehr verehrten Damen und Herren, an dieser Stelle möchte ich Sie alle einladen, sich in der Allianz für Cyber-Sicherheit zu engagieren. Hier finden Sie ein großes Angebot an Informationen zu Schutzmaßnahmen und Hilfestellungen.

Seit 2010 arbeiten der Bund, die Länder und Kommunen im IT-Planungsrat zusammen. Dem IT-Planungsrat gehören als Mitglieder die Beauftragte der Bundesregierung für Informationstechnik sowie jeweils ein für Informationstechnik zuständiger Vertreter jedes Landes an. Neben den Mitgliedern nehmen an den Sitzungen drei Vertreter der Gemeinden und Gemeindeverbände, die von den kommunalen Spitzenverbänden auf Bundesebene entsandt werden, und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beratend teil. Der Vorsitz wechselt jährlich zwischen Bund und Ländern. Für 2013 hatte ihn der Freistaat Bayern übernommen. Der Auftrag des IT-Planungsrates besteht darin, die Zusammenarbeit in der IT und im e-Government von Bund, Ländern und Kommunen verbindlich zu gestalten. Ziele sind nutzerorientierte elektronische Verwaltungsdienste und ein wirtschaftlicher, effizienter und sicherer IT-Betrieb der Verwaltung.

Der IT-Planungsrat hat sich auf seiner CeBIT-Sitzung im März 2013 mit Maßnahmen befasst, die einen gemeinsamen Rahmen für

Bund, Länder und Kommunen zum Auf- und Ausbau des Informationssicherheitsmanagements in der öffentlichen Verwaltung abstecken, die Netzinfrastrukturen absichern sowie einheitliche Sicherheitsstandards für ebenenübergreifende IT-Verfahren festlegen.

Die Ergebnisse sind in einer „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ zusammengestellt, die ebenfalls im März beschlossen wurde.

Im Umsetzungsplan ist unter anderem die Einrichtung einer dauerhaften Bund-Länder-Arbeitsgruppe Informationssicherheit vorgesehen. Die Arbeitsgruppe setzt sich aus den benannten Vertretern der Mitglieder des IT-Planungsrats zusammen und erarbeitet gemeinsam Vorschläge zur Weiterentwicklung der Leitlinie sowie einen jährlichen Bericht an den IT-Planungsrat. Sie dient außerdem dem regelmäßigen Austausch zu Themen der Informationssicherheit unterhalb des IT-Planungsrats.

Ich fordere Sie als Vertreter von Kommunen, Gemeinden und Ländern ausdrücklich zur Umsetzung der beschlossenen „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ auf, damit auch die IT-Systeme der Städte und Gemeinden das gleiche Sicherheitsniveau wie die IT-Systeme auf Landes- und Bundesebene erreichen.

Ein weiteres Projekt, mit dem sich der IT-Planungsrat beschäftigt, ist die Einführung von De-Mail. Durch den Einsatz von De-Mail in Verbindung mit dem neuen Personalausweis in den Verwaltungen wird der gesetzlichen Forderungen nach Schriftform Genüge getan. Dadurch werden Vorgänge, die vom Antragsteller bislang persönlich zu unterschreiben sind, einer digitalen Bearbeitung zugänglich. Dies wird eine Arbeitserleichterung für uns alle, sowohl auf der Nutzer- als auch auf der Bearbeiterseite, sein. Durch die Verkündung des E-Government-Gesetzes am 31. Juli 2013 kann die Identifizierungsfunktion des neuen Personalausweises nun in elektronischen Verfahren eingesetzt werden – auch dort, wo Schriftform gefordert wird. Bei De-Mail wird dies am 1. Juli 2014 der Fall sein.

Die Zusammenarbeit zum Schutz des Cyber-Raums – und das macht das zu Beginn angesprochene Beispiel deutlich – kann nicht an den Grenzen Deutschlands enden. Das effektive Zusammenwirken für Cyber-Sicherheit muss in Europa und weltweit organisiert werden. Auch dieses Ziel wurde bereits in der Cyber-Sicherheitsstrategie definiert.

Die Bundesregierung engagiert sich insbesondere bei den Aktivitäten zur Erhöhung der Cyber-Sicherheit auf EU-Ebene.

So hat die EU-Kommission gemeinsam mit dem Europäischen Auswärtigen Dienst Anfang dieses Jahres eine Cybersicherheitsstrategie und dem Europäischen Parlament und dem Rat einen Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union vorgelegt. Die Anwendung der Richtlinie ist auch für Verwaltungen vorgesehen. Die Bundesregierung lehnt dies ebenso wie der Bundesrat mit dem Argument der Subsidiarität ab. Aber das Ziel, die IT der Verwaltungen sicherer zu machen, ist grundsätzlich zu begrüßen.

Bei der Abstimmung dieser Papiere bringen wir deutsche Erfahrungen aus der Umsetzung der nationalen Cyber-Sicherheitsstrategie aktiv ein.

International engagieren wir uns noch im Rahmen der NATO-Cyberabwehrstrategie und für Verhaltensregeln für Staaten im Cy-

ber-Raum, die sogenannten „Norms of State Behaviour in Cyber-Space“ in einer Expertengruppe der Vereinten Nationen.

Mit der Verabschiedung der Cyber-Sicherheitsstrategie für Deutschland kam die Bundesregierung ihrer Verantwortung zur Verbesserung der IT-Sicherheit in Deutschland nach.

Die national und international geführten Diskussionen zeigen, dass wir damit den richtigen Weg beschritten haben. Andere Staaten orientieren sich in ihren Überlegungen an den Maßnahmen Deutschlands. Die Notwendigkeit zur Sensibilisierung für das Thema Cyber-Sicherheit nimmt allenthalben zu. So war es auch ein ganz wichtiger Schritt, die Allianz für Cyber-Sicherheit ins Leben zu rufen. Es liegt in unser allem Interesse, wenn Sie sich als Betreiber Kritischer Infrastrukturen am Umsetzungsplan KRITIS beteiligen und als Verwaltung die Möglichkeit nutzen, der Allianz für Cyber-Sicherheit beizutreten.

.

Bei allen Bemühungen muss festgehalten werden: Der Bund allein kann Cyber-Sicherheit nicht gewährleisten; auch Kommunen, Länder und die Wirtschaft sind aufgerufen, ihren Beitrag zu leisten.

Cyber-Sicherheit kann nur in einem umfassenden, kooperativen Ansatz verfolgt werden, der alle Akteure einbezieht. Wir brauchen ein Zusammenspiel aller gesellschaftlichen Gruppen und eine gemeinsame Übernahme von Verantwortung.

Ich danke für Ihre Aufmerksamkeit.

Cornelia Rogall-Grothe *ist Staatssekretärin im Bundesministerium des Innern und Beauftragte der Bundesregierung für Informationstechnik*

Informationstechnik krisenfest machen

Reinhold Harnisch

Durch die Entwicklungen und Trends in der Gesellschaft, Wirtschaft und öffentlichen Verwaltung wie Zentralisierung, wachsende Globalisierung und zunehmende Vernetzung sind die möglichen Bedrohungen der Informationstechnik stark angestiegen. Die zusätzlich steigende Komplexität der Geschäftsprozesse und die wachsende Bedeutung der Informationstechnik lassen Ausfälle schnell große Auswirkungen auf diese Institutionen oder auf ganze Regionen haben.

Das Kommunale Rechenzentrum Minden-Ravensberg/Lippe (krz) etablierte 2009 ein Notfallmanagement nach BSI-Standard 100-4, um diesen Risiken Rechnung zu tragen. Das krz, das als erster kommunaler Service-Provider in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz zertifiziert wurde, betreut in seinem Verbandsgebiet drei Kreise, 34 Städte und Gemeinden mit ca. 900.000 Einwohnern. Darüber hinaus nutzen ca. 600 kommunale Anwender in vierzehn Bundesländern die Leistungen des Lemgoer Service-Providers. Das krz ist eine Körperschaft des öffentlichen Rechts in der Form eines kommunalen Zweckverbandes mit mehr als 200 Mitarbeiter/-innen und über 40 Jahren Erfahrung im IT-Bereich.

IT krisenfest machen – brauchen wir das überhaupt?

Die öffentliche Verwaltung, aber auch die Wirtschaft unterliegt aktuell starken Sparzwängen. Deshalb werden die Aufgabengebiete IT-Sicherheit und Notfallvorsorge/-bewältigung oft als „Ressourcenfresser“ bezeichnet, die keine zusätzlichen Einnahmen erwirtschaften. Investitionen werden, wenn überhaupt, nur im geringen Maße getätigt, vornehmlich im Bereich der Informationssicherheit. Das Notfallmanagement wird monetär eher stiefmütterlich behandelt. Bei Vielen gilt das Sprichwort „Uns ist doch noch nie etwas passiert“.

Unter Berücksichtigung der Bedrohungen, Eintrittswahrscheinlichkeiten und mögliches Ausmaß von Schäden wird oft klar, dass es zu viele unbekannte Größen gibt, um eine Entscheidung für oder gegen Investitionen zu treffen. Um diese Größen zu bestimmen und geeignete Maßnahmen zu entwickeln, wird ein Notfallmanagement benötigt, damit das mögliche Ausmaß direkter und indirekter Schäden abgeschätzt, Eintrittswahrscheinlichkeiten bestimmt und mögliche Risiken identifiziert werden können. Die daraus abgeleiteten Maßnahmen lassen sich oftmals ohne großen Einsatz von Ressourcen umsetzen.

Das Notfallmanagement kann in die Bereiche Notfallvorsorge und Notfallbewältigung unterteilt werden. Die Notfallvorsorge ist proaktiv tätig, die Notfallbewältigung reaktiv.

Die Notfallvorsorge hat das Ziel, die Krisenschwelle der Institution zu erhöhen. Dazu werden vorbeugende Maßnahmen entwickelt, die den Schaden und die Eintrittswahrscheinlichkeit von Risiken reduzieren und ein schnelles und sinnvolles Reagieren auf einen Vorfall ermöglichen.

Da nicht alle Risiken durch Sicherungsmaßnahmen vollständig eliminiert werden können, wird dem verbleibenden Restrisiko durch eine Notfallbewältigung begegnet.

Das Ziel der Notfallbewältigung ist es, Notfall- und Krisensituationen zu identifizieren und zu analysieren, Bewältigungsstrategien zu entwickeln sowie Gegenmaßnahmen einzuleiten und zu verfolgen.

Um die Widerstandsfähigkeit einer Institution und die Robustheit der Geschäftsprozesse zu erhöhen, ist es von fundamentaler Bedeutung, beide Gebiete zu betrachten und sich in der Konsequenz mit folgenden exemplarischen Fragestellungen auseinanderzusetzen:

- Welche direkten oder indirekten Schäden entstehen, wenn z. B. ein Gebäude, ein Geschäftsprozess oder eine Anwendung ausfällt?
- Kann ein Ausfall rechtliche Konsequenzen oder Imageschäden zur Folge haben?
- Welche Eintrittswahrscheinlichkeiten haben die unterschiedlichen Szenarien?
- Welche Maßnahmen wurden für die Notfallprävention umgesetzt?
- Was wird für die Notfallbewältigung getan? Gibt es einen Alarmierungsplan, definierte Meldewege und ein Rollenkonzept?
- Wann müssen die ausgefallenen Systeme wieder funktionsfähig sein?
- Gibt es einen Wiederanlaufplan zum Wiederherstellen von Geschäftsprozessen oder Anwendungen?

Ziel ist es, sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz auch bei einem großen Schadensereignis gesichert ist. Insbesondere die öffentliche Hand ist aufgrund der Daseinsvorsorge angehalten, sich mit einem Notfallmanagement auseinanderzusetzen.

Die wichtigsten Sicherungsmaßnahmen sind gut ausgebildete und motivierte Mitarbeiterinnen und Mitarbeiter in Sicherheitsfragen.

Ebenso sind technische Sicherheitsmaßnahmen von Bedeutung: beispielsweise sollten Notstromaggregate eingesetzt und ein 2-Häuser-Konzept (redundante Haustechnik und IT-Komponenten) entwickelt werden. Abschließend sollten mit Hilfe von Notfallübungen, z. B. Stabsrahmenübungen oder Wiederanlauf nach Ausfall eines Geschäftsprozesses oder einer Anwendung, die etablierten organisatorischen und technischen Sicherheitsmaßnahmen überprüft werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit dem Standard 100-4 „Notfallmanagement“ ein Rahmenwerk an, das die Einführung eines Notfallmanagement sowohl in eine kleine als auch in eine große Institution beschreibt.

Wie kann die Grundversorgung abgesichert werden?

Die konkreten Bedrohungslagen wie Pandemien, flächendeckende und lang anhaltende Stromausfälle, Terrorangriffe oder Extremwetterereignisse erfordern eine veränderte Denkweise und neue Technologien, die eine vernetzte Sicherheit generieren.

Die aktuellen Ereignisse aus dem Jahr 2013 – der Brand in der Vermittlungsstelle der Telekom in Siegen oder die Hochwasserkatastrophe im Süden und Osten der Republik – zeigen, dass es sinnvoll ist, nicht nur die eigene Institution zu betrachten, sondern im Bereich der Grundversorgung (Strom, Wasser, Datennetz, etc.) überregional zusammen zu arbeiten.

Am 21. Januar 2013 brannte die Vermittlungsstelle in Siegen. Dadurch wurde ein großflächiger Ausfall der Notrufe 110 und 112 sowie der Telefonie, des Internets, des lokalen Radios und des D1-Mobilfunknetz verursacht. Die Banken und Sparkassen mussten den Betrieb einstellten, Geldautomaten und Kassensysteme fielen aus, Lebensmittelgeschäfte mussten schließen, Krankenhäuser mussten Operationen verschieben und Hausnotrufe waren nicht funktionsfähig. Betroffen waren ca. 500.000 Haushalte in den Kreisen Siegen-Wittgenstein, Marburg-Biedenkopf, Lahn-Dill und Altenkirchen. Der wirtschaftlicher Schaden wird laut IHK auf 10 Mio. € geschätzt.

Der Brand in einer von 80 zentralen Telekommunikations-Vermittlungsstellen hat nicht vorhersehbare Auswirkungen gezeigt, so dass zeitweilig alle überregionalen Leitungen ausgefallen sind – von allen Providern. Hinzu kam ein Ausfall der meisten wesentlichen Verwaltungsverfahren bzw. -einrichtungen:

- Bürgerämter (Einwohner- und Meldewesen),
- Straßenverkehrsämter (Kfz-Zulassung und Führerschein),
- Sozialämter,
- Personalverwaltung,
- Finanzbuchhaltung und kommunale Kassen sowie
- Steuerämter.

Somit war kein normaler Dienstbetrieb der öffentlichen Verwaltung in Südwestfalen möglich. Ohne das Kommunale Richtfunknetz der Kreise Olpe und Siegen-Wittgenstein hätten die Städte und Gemeinden vier Tage keine Verbindung zur Datenzentrale und keinen Zugang zu den zentralen Verwaltungsverfahren gehabt, da der Internet-Zugang der Telekom bis zum 24. Januar 2013 gestört blieb.

Der Brand hat beispielhaft gezeigt, dass es nicht mehr ausreicht, sich als einzelne Behörde oder einzelnes Wirtschaftsunternehmen abzusichern. Vielmehr müssen sie sich mit überregionaler Sicherheit befassen.

Als Beispiel: Der Betrieb von parallelen Netz-Zugängen über mehrere Provider ist zwar wichtig, allerdings hat das Ereignis gezeigt, dass viele die gleiche Infrastruktur nutzen. Hier ist es sinnvoll, dass die betroffenen Institutionen in Zusammenarbeit mit der Kommunikationsgesellschaft Lösungen finden.

Dass das überregionale Zusammenarbeiten im Bereich Notfallmanagement und Katastrophenschutz oder auch IT-Sicherheit sinnvoll ist, zeigt z. B. die vom BSI gegründete Allianz für Cyber-Sicherheit oder das Warn- und Informationssystem KATWARN. Letzteres wurde vom Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS entwickelt und von den öffentlichen Versicherern Deutschlands beauftragt (www.katwarn.de). KATWARN ist ein Warnsystem, das individuell über Gefahren wahlweise per SMS, E-Mail und Smartphone-Applikation informiert und den Betroffenen Anweisungen zum „besten Verhalten“ gibt. Darüber hinaus nutzt der Deutsche Wetterdienst das System mit bundesweiten Unwetterwarnungen der höchsten Stufe, bei Unwetterereignissen mit weiträumigen und extremen Gefahren. Zurzeit wird

KATWARN DAS KOMMUNALE WARN- UND INFORMATIONSSYSTEM FÜR DIE BEVÖLKERUNG

das Warn- und Informationssystem von 17 Kreisen und Städten genutzt.

Fazit – Was bleibt übrig?

Es genügt nicht allein, die eigene Institution zu sichern. Die „lokale“ IT-Sicherheit und das eigene Notfallmanagement sind die Grundlagen, die geschaffen werden müssen, damit die übergreifende Sicherheit erreicht werden kann. Bedeutet: „Vorsorge statt Nachsorge!“

Sichere kommunale Rechenzentren, die mit einem Backup-Rechenzentrum und redundanten Infrastrukturen ausgestattet sind, können Ausfälle und damit verbundene Schäden zwar nicht verhindern, jedoch effizient vermindern oder begrenzen. Die Rechenzentren müssen sich auf dem höchstmöglichen Sicherheits-Standard befinden, um auf die möglichen Risiken vorbereitet zu sein. Das Bewusstsein für die Notwendigkeit von präventiven Maßnahmen muss verankert werden.

Machen wir uns gemeinsam auf: Auf den Weg zur sicheren Kommune.

Reinhold Harnisch *ist Geschäftsführer des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe (krz), Lemgo und stellvertretender Vorstandsvorsitzender der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V. VITAKO, Berlin*

Woran erkennt man eine Katastrophe? Wie muss sich die Kommune darauf vorbereiten?

Albrecht Broemme

1. Einleitung

Deutschland war in den vergangenen Jahren relativ selten von Großschadensereignissen betroffen. Das diesjährige Hochwasser an Elbe und Donau samt deren Nebenflüssen zeigt, dass auch hierzulande mit Katastrophen zu rechnen ist und diese vor allem hohe Sachschäden verursachen. Die Medien berichteten über (vermeintliche) Defizite des Hochwasserschutzes, zeigten spektakuläre Bilder und berichteten über die tragischen Schicksale der Opfer. Die eingesetzten Organisationen kamen – trotz des Ausmaßes des Hochwassers – auf ein differenzierteres, weniger dramatisches Bild. In der Gesamtschau kann durchaus positiv Bilanz gezogen werden: Vieles ist insbesondere seit dem letzten Hochwasser 2002 verbessert worden. Allerdings bleibt noch genug zu tun.

Extreme Wetter- und Naturereignisse werden auch in Deutschland immer öfter zu immer größeren Schadensereignissen führen. Dies liegt zum einen an einer höheren Frequenz herausragender Wetter- und Naturereignisse wie beispielsweise Starkniederschläge, Hitze- und Kälteperioden, zum anderen in der zunehmenden Verletzbarkeit der globalisierten Gesellschaft. Dies wird durch ein allgemein ausgeprägtes mangelndes Risiko-Bewusstsein noch verstärkt.

2. Katastrophe und Katastrophenschutz

Nach der Definition der Vereinten Nationen ist eine Katastrophe „die Unterbrechung der Funktionsfähigkeit einer Gemeinschaft oder Gesellschaft, die hohe menschliche, materielle, ökonomische und ökologische Verluste verursacht und die Fähigkeit der betroffenen Gemeinschaft oder Gesellschaft übersteigt, diese aus eigener Kraft zu bewältigen.“ Eine Katastrophe betrifft also meistens viele Menschen, sie schädigt die Lebensgrundlagen und Sachwerte auch langfristig und kann den Zusammenbruch der kritischen Infrastrukturen zur Folge haben (und umgekehrt).

Um Leben, Gesundheit oder die Umwelt vor Katastrophen zu schützen, sind präventive Maßnahmen am wirksamsten. Der Katastrophenschutz dient „nur“ der Gefahrenabwehr, also der Bekämpfung von Katastrophen. Er liegt in der Verantwortung der Kommunen, Kreise und Länder. Im Katastrophenschutz sollen alle an der Gefahrenabwehr beteiligten Behörden, Organisationen und Einrichtungen unter einheitlicher Führung durch die örtlich zuständige Katastrophenschutzbehörde zusammenarbeiten.

Der Bevölkerungsschutz in Deutschland gilt vielen Staaten als Vorbild. Er basiert ganz überwiegend auf ehrenamtlichem Engagement. Außerhalb der Ballungsräume gibt es überwiegend freiwillige Einsatzkräfte, ergänzt durch Hauptamtliche. In Großstädten ist es prinzipiell umgekehrt, d.h. der Katastrophenschutz wird hier von Hauptamtlichen dominiert.

3. Aufgaben der Kommunen

Die Katastrophenschutzbehörden der Kommunen, Kreise und kreisfreien Städte haben die Aufgabe, mögliche Katastrophen rasch zu erkennen und eingetretene Schadenslagen zu bekämpfen. Hierfür ist eine umfassende Planung und Vorbereitung zwingend erforderlich. Bestenfalls werden schon im Vorfeld die örtlich bestehenden Risiken z.B. durch exponierte Lage an Flüssen, Industrieanlagen und gegebenenfalls zu erwartende Schadenspotentiale identifiziert. Eine sinnvolle Vorbereitung besteht nicht nur aus reaktiven Maßnahmen zur Bewältigung von Katastrophen, sondern umfasst auch präventive Maßnahmen der Vorbeugung, der Frühwarnung und der Information.

Auch bei „perfekten“ präventiven Maßnahmen lassen sich Katastrophen nicht verhindern – die Auswirkungen sind jedoch dann wesentlich geringer. Es gilt der Grundsatz:

Ein Euro investiert in die Prävention erspart sieben Euro bei Schäden.

Auf kommunaler Ebene müssen Notfallplanungen erstellt und geübt werden. Sie sollen Routinen entwickeln, Entscheidungswege definieren und die Zusammenarbeit der verschiedenen Akteure im Vorfeld definieren.

Trotz dieser Planungen ist der Anfang einer Katastrophe meist durch eine Phase gekennzeichnet, in der gewissermaßen Chaos herrscht und die vorhandenen Planungen, soweit sie vorliegen, mit den vorhanden Ressourcen und Möglichkeiten kollidieren. Optimal geschulte und besetzte Krisenstäbe müssen dann eine Abschätzung der Situation vornehmen, die bestmögliche Lösung zu finden und umzusetzen. Die Stäbe kennen die verfügbaren Ressourcen, die zu berücksichtigenden Hierarchien sowie die notwendigen Zuständigkeiten und Verantwortlichkeiten.

4. Wie kann das THW helfen?

Das Technische Hilfswerk (THW) ist eine nicht rechtsfähige Bundesanstalt im Geschäftsbereich des Bundesministeriums des Innern.

Es gibt Deutschlandweit 668 THW Ortsverbände, in denen über 80.000 ehrenamtlichen Helferinnen und Helfer engagiert sind. Diese werden von rund 800 Hauptamtlichen in 66 Geschäftsstellen, in acht Landesverbänden, in der THW-Bundesschule mit zwei Standorten, im Zentrum für Auslandslogistik (ZAL) sowie zehn Fachreferaten in der THW Leitung unterstützt.

Das THW wurde 1950 gegründet. Organisation, Aufgaben und Befugnisse des THW sind in einem eigenen Gesetz zuletzt 2009 definiert:

Nach § 1 II Nr. 3 THW-Gesetz kann das THW im Katastrophenfall, bei öffentlichen Notständen und Unglücksfällen größeren Ausmaßes von den Kommunen angefordert werden. Für die örtliche Gefahrenabwehr (unterhalb der Katastrophe) steht das THW nach den Grundsätzen der allgemeinen Amtshilfe gemäß den Vorschriften des Verwaltungsverfahrensgesetzes (§ 4 ff. VwVfG) zur Verfügung. Derartige Anforderungen können an jede Ebene des THW gerichtet werden, d.h. an den Ortsbeauftragten oder den Geschäftsführer, den Landesbeauftragten oder an die THW-Leitung.

Die seit Februar 2013 in Kraft gesetzte neue Verordnung des THW hat zum Ziel, die Abrechnung zwischen THW und Anforderern bei gleichzeitig höherer Rechtssicherheit zu vereinfachen.

Im Einsatz werden die THW-Einheiten prinzipiell der örtlichen Einsatzleitung unterstellt und erhalten von dieser ihre Einsatzaufträge. In der Regel obliegt die Einsatzleitung der Feuerwehr. Jedoch übertragen Gefahrenabwehrbehörden oder andere Stellen dem THW oft fachlich oder räumlich abgeschlossene Aufgaben, die es hinsichtlich Führung, Taktik, Technik und Logistik eigenständig löst.

Die Verbindung zwischen den planerisch und vorsorgend tätigen Verwaltungsebenen und der operativen Einsatztätigkeit vor Ort ist im THW durch die Einrichtung von Leitungs- und Koordinierungsstäben auf allen Ebenen geregelt, die lageangepasst die Kommunikation mit den Verwaltungsebenen von Bund, Ländern und Kommunen aufrechterhalten.

Das THW plant anhand von Szenarien und verfügt über vielfältige Einsatzmöglichkeiten. Für den Einsatz stehen in jedem Ortsverband ein technischer Zug, bestehend aus Zugtrupp, zwei Bergungsgruppen und mindestens einer Fachgruppe zur Verfügung. Die Bergungsgruppen sind mit ihrem Personal und der Ausstattung in der Lage, die Kernkompetenzen des THW in einem breiten Aufgabenspektrum abzudecken, d.h. zu retten, zu bergen, Sicherungs- und leichte Räumarbeiten vorzunehmen sowie technische Hilfe zu leisten. Die bundesweit einsatztaktisch dislozierten THW-Fachgruppen ergänzen und erweitern das Spektrum qualitativ und quantitativ in folgenden Bereichen:

Die technische Hilfe im Bereich der (kritischen) Infrastrukturen beinhaltet die Fachgruppen Elektroversorgung, Trinkwasserversorgung und Brückenbau. Die Fachgruppe Brückenbau kann beispielsweise kurzfristig Brücken aus vorgefertigten Teilen oder herkömmlichen Baumaterialien wie Holz oder Stahl bis zu einer Länge von 50 Metern errichten. Seit 2010 kann das THW auch Eisenbahn-Behelfsbrücken bis 120 Meter Länge errichten.

Im Bereich der Technischen Gefahrenabwehr werden Ortung-, Rettungs- und Bergungsarbeiten durchgeführt: Die Fachgruppe Ortung setzt Rettungshunde und technische Ortungsgeräte zur Lokalisierung von eingeschlossenen oder verschütteten Menschen ein. Rettungs- und Bergungsarbeiten werden wie bereits oben beschrieben über die Bergungsgruppen abgedeckt.

Die Fachgruppe Räumen verfügt über leistungsfähige Baumaschinen, räumt die Schadensstellen, legt Zu- und Abfahrtswege an, hebt Gräben und Abflüsse aus und zerkleinert Hindernisse und Trümmer. Die Fachgruppe Sprengen unterstützt Einsätze und beseitigt Gefahren mit Hilfe von Sprengungen.

Die Fachgruppe Beleuchtung verfügt über eine breite Palette von Beleuchtungsmitteln. Damit lassen sich insbesondere bei größeren Schadensereignissen weite Strecken und große Flächen ausleuchten.

Die Fachgruppen Wassergefahren und Wasserschaden/Pumpen kommen mit ihren unterschiedlichen Aufgabenspektren bei Überflutungen und Überschwemmungen zum Einsatz.

Für umfassende Dienstleistungen für die THW-Einheiten im Einsatz stehen die Fachgruppen Führung/Kommunikation z.B. für das Einrichten und Betreiben von Führungsstellen, Führungsunterstützung, Einrichtung temporärer Telekommunikationssysteme, und Logistik, für das Einrichten und Betreiben von Logistikstützpunkten, und die Verpflegung und Betreuung der Einsatzkräften zur Verfügung. Ebenso werden die Materialerhaltung,

Reparatur- und Wartungsarbeiten für Einsatzausstattung, Verbrauchsgütertransport für Einsatzbedarf sichergestellt.

Technische Hilfe leistet das THW auch im Bereich Umweltschutz z.B. bei der Ölschadenbekämpfung und mittels Wasseranalysen und Abwasserentsorgung.

Die Errichtung und Einrichtung von Notunterkünften und Sammelplätzen mit entsprechender Infrastruktur gehört ebenso zum Aufgabenportfolio wie weitere technische Hilfeleistungen auf Verkehrswegen, Höhenrettung, Tauchen und der behelfsmäßige Straßenbau.

Es besteht für die zuständigen Stellen der Länder und Kommunen zudem immer die Möglichkeit, sowohl im Rahmen der konkreten Einsatzvorbereitung als auch im Vorfeld, fachliche Beratung des THW in Anspruch zu nehmen. Die THW-Fachberater unterstellen sich dann in der Regel für die Zeit der Inanspruchnahme den zuständigen Stellen.

Das THW hat eigens für die Zusammenarbeit mit Anforderern, auch auf landes- bzw. kommunaler Ebene, eine Broschüre erstellt, aus der u. a. anhand von Kurzbeschreibungen die THW-Einsatzoptionen einfach und im Überblick zu entnehmen sind.

5. Ausblick

Die für den Bevölkerungsschutz verfügbaren Akteure sind ebenso vielfältig wie leistungsstark. Deren Zusammenarbeit ist oftmals ebenso facettenreich. Die Kenntnis der eigenen Ressourcen, Fähigkeiten und Grenzen sowie die der anderen Organisationen ist eine wichtige Voraussetzung für eine gute Zusammenarbeit. Man darf „die Visitenkarten nicht erst auf dem Trümmerkegel austauschen“. Die Katastrophenschutzplanung, die Aus- und Fortbildung der Einsatzkräfte, regelmäßige organisations- und bundeslandübergreifende Übungen sind die Voraussetzung für die Bewältigung von Großschadensereignissen. Informationsflüsse, Meldewege und Schnittstellen auf regionaler und überregionaler Ebene müssen bekannt sein und regelmäßig getestet werden.

Ein Aspekt, der beim letzten Hochwasser in den Fokus geriet, ist die erfreuliche Bereitschaft vieler Menschen, sich über soziale Netzwerke zu organisieren, um Hilfe zu leisten. Hierdurch ergibt sich ein kurzfristig verfügbares interessantes Potential, das kanalisiert und angeleitet werden kann. Die Selbsthilfefähigkeit der Gesellschaft ist und bleibt von grundlegender Bedeutung. Sie wird über die aktive Auseinandersetzung der Bevölkerung mit der Thematik ausgebaut und kann einen entscheidenden Beitrag zu Widerstandfähigkeit einer Gesellschaft leisten.

Je besser die Kommunalen „ihren“ Katastrophenschutz „im Griff haben“, desto besser ist die Bevölkerung insgesamt geschützt.

Albrecht Broemme *ist Präsident der Anstalt Technisches Hilfswerk THW, Berlin.*

Zentrale Koordinierungsstelle zum Schutz Kritischer Infrastrukturen (KoSKI) in Rheinland-Pfalz

Gerd Gräff

Ihre Einladung, die neu eingerichtete Zentrale Koordinierungsstelle zum Schutz Kritischer Infrastrukturen in Rheinland-Pfalz vorzustellen, habe ich gerne angenommen, zumal diese Fragen in Zukunft noch stärker als bisher im Fokus aller öffentlichen und privaten Sicherheitspartner stehen werden.

Großflächige Stromausfälle verdeutlichen immer wieder, wie empfindlich Kritische Infrastrukturen als Lebensadern unserer modernen Gesellschaft sind. Dies haben die Hochwasserkatastrophen der letzten Wochen, unter anderem in Passau, wieder einmal gezeigt.

Wenn solche Systeme gestört werden, kann das öffentliche Leben nur noch schwer aufrechterhalten werden. Dies gilt sowohl für die Technischen Basisinfrastrukturen, wie

- Energieversorgung,
- Informations- und Kommunikationstechnologie,
- Transport- und Verkehr,
- Trinkwasserversorgung und Abwasserentsorgung,

als auch für die sozioökonomischen Dienstleistungsinfrastrukturen wie

- Ernährung,
- Gesundheitswesen,
- Brand- und Katastrophenschutz, Rettungsdienst,
- Parlament, Regierung, öffentliche Verwaltung, Justiz,
- Finanz- und Versicherungswesen,
- Medien und Kulturgüter.

Die Ursachen für Störungen können vielfältig sein, von Naturkatastrophen bis hin zu Sabotageakten. Dabei können schon kleine Ursachen große Wirkung haben. So hat ein Brand in einer Vermittlungsstelle eines Telekommunikationsunternehmens Anfang des Jahres in Siegen zu einem großflächigen Ausfall von Festnetz-, Internet- und Mobilfunkdiensten geführt. Rund 90.000 Kunden konnten zeitweise weder telefonieren noch Notrufe absetzen.

Gerade wegen dieser weitreichenden Auswirkungen von Störungen ist der Schutz Kritischer Infrastrukturen eine wichtige Aufgabe vorsorgender Sicherheitspolitik.

Die Landesregierung von Rheinland-Pfalz hat diesem Thema schon frühzeitig eine besondere Priorität eingeräumt. So haben wir nach den Terroranschlägen vom 11. September 2001 in einer ressortübergreifenden Sicherheits-Arbeitsgruppe unter Einbeziehung aller Sicherheits- und Fachbehörden ein umfassendes Sicherheitskonzept für besonders störanfällige Infrastrukturen erstellt.

Dabei haben wir nicht nur staatliche Einrichtungen in die Vorsorgemaßnahmen einbezogen. Wichtig erschien uns von Anfang an, auch private Betreiber Kritischer Infrastrukturen einzubinden, angefangen von Flughäfen über Energieversorgungseinrichtungen, Pipelines bis hin zu Pharma- und Chemieunternehmen.

Kritische Infrastrukturen werden vermehrt von privatwirtschaftlichen Betreibern wahrgenommen. Gerade in Krisensituationen ist der Staat daher auf eine große Transparenz und Einbindung dieser Betreiber in die erforderlichen Entscheidungen angewiesen.

Eine weitere Initialzündung war ein großflächiger Stromausfall in der Region Trier/-Luxemburg im Jahr 2004. Ein Kurzschluss in einer Versorgungsleitung des europäischen Verbundnetzes hatte zum Zusammenbruch aller untergeordneten Systeme geführt. Stundenlang musste rund eine Million Menschen ohne Strom auskommen.

Diesen Zwischenfall haben wir zum Anlass genommen, die Zusammenarbeit mit den Elektrizitätsversorgungsunternehmen noch weiter zu intensivieren. Dabei haben wir auch die Erkenntnisse des Stromausfalls im Münsterland ein Jahr später mit einbezogen.

Im Rahmen dieses vorbildlichen Beispiels öffentlich-privater Partnerschaft haben wir unter anderem vereinbart, dass ein regelmäßiger Erfahrungsaustausch zwischen den Sicherheitsbehörden und den Stromversorgern – auch ohne konkreten Anlass – stattfindet.

Sehr wichtig erscheinen uns auch strukturierte Meldewege und -verfahren, auch über redundante Verbindungen wie etwa Satellitentelefone, denn der Informationsfluss muss auch gewährleistet sein, wenn die üblichen Kommunikationsnetze nicht mehr funktionieren.

Dazu werden Zuständigkeiten und Verantwortlichkeiten für die vier Handlungsphasen der Krisenkommunikation klar definiert, nämlich die potenzielle Krisenphase, die latente Krisenphase, die akute Krisenphase und die Nachkrisenphase.

So melden die Elektrizitätsversorgungsunternehmen in Rheinland-Pfalz jeden Stromausfall, der voraussichtlich länger als zwei Stunden dauert und mehr als 3.000 Personen betrifft, nicht nur den verantwortlichen kommunalen Stellen, sondern auch dem Lagezentrum des Innenministeriums.

Auch die kommunalen Aufgabenträger sind auf einen großflächigen Stromausfall vorbereitet. So haben die meisten von ihnen eine mit den Energieversorgern erarbeitete Checkliste umgesetzt, in der viele Vorsorgemaßnahmen festgelegt sind, von denen ich nur beispielhaft erwähnen möchte:

- Sicherstellung der Ersatzstromversorgung in Verwaltungsgebäuden, Feuerwachen, Bürgerhäusern und anderen Einrichtungen,
- Ermittlung von Tankstellen mit Notstrom-Einspeisemöglichkeit und vertragliche Vereinbarung mit den Betreibern über die vorrangige Bedienung des Katastrophenschutzes,
- unverzügliche Besetzung von Feuerwehrhäusern als Ansprechstelle für die Bevölkerung und zum Absetzen von Notrufen,
- verstärkte Information der Bevölkerung über Selbsthilfemaßnahmen.

Aber auch in anderen Bereichen sind wir gut aufgestellt, etwa bei der Abwehr von Sabotageangriffen auf Kritische Infrastrukturen.

Die Strukturen sind immer stärker miteinander verwoben. So ist der Telekommunikationssektor unmittelbar mit dem Energiesektor verbunden. Telekommunikation benötigt Energie. Energienetze werden durch Mittel der modernen Kommunikation gesteuert.

Im Krisenfall gilt es eine Flut von Informationen, sowohl räumlich als auch zeitlich, zu bewerten. Informationsmanagement mit dem Ziel, valide Informationen für eine verantwortliche Krisenkommunikation bereitzustellen und ggf. sogar verfälschte und gefälschte Informationen zu finden, ist eine besondere Herausforderung.

Cyberangriffe, ausgeführt durch Hacker, Cyber-Kriminelle oder staatliche Aggressoren, können auch Krisen bei Kritischen Infrastrukturen auslösen. Durch die unberechtigte Nutzung von Fernwartungszugängen, menschliches Fehlverhalten, Einschleusen von Schadcodes über Wechselmedien, um nur einige Beispiel zu nennen, werden Bedrohungen in beliebigen Kritischen Infrastrukturen ausgelöst. Die weitere Bewertung der einzelnen Angriffe, insbesondere die Täteridentifikation, obliegt dann in Abhängigkeit der Art des erfolgten Angriffs den Polizeibehörden oder Nachrichtendiensten.

So ist über eine Routinewartung bei zwei US-amerikanischen Stromversorgern Ende 2012 jeweils ein mehrwöchiger Ausfall zweier Elektrizitätswerke eingetreten. Immer wieder sind Banken und Aktienmärkte Ziel von Angriffen aus dem Internet. Motive und Aufwand dieser Angriffe lassen dabei vermehrt auf gezielte Angriffe, ja sogar auf skalpellartige Angriffe auf bestimmte Strukturen und Einrichtungen schließen. Hierbei ist die gezielte Sabotage spezieller IT-Systeme mit einem großen Schadensausmaß das Ziel der Angreifer.

Aufgrund der komplexen Systemstruktur von Informations- und Telekommunikationstechnik und ihrer starken Abhängigkeit von der Stromversorgung können die Auswirkungen von Stromausfällen gravierend sein. Innerhalb der Kommunikationsnetze können hierbei besondere Netzknoten oder Steuerungseinheiten ausfallen.

Da durch den Ausfall von Kommunikationsnetzen auch das Krisenmanagement von Behörden und Krisenstäben massiv eingeschränkt wird, hat das Land Rheinland-Pfalz für diesen Fall Vorsorge getroffen. Zur weiteren Katastrophenvorsorge werden neuralgische Standorte des Landes über redundante und mit eigener netzunabhängiger Stromversorgung betriebene Funkverbindungen miteinander verbunden. Hierdurch steht ein zweites unabhängiges Netz zur Verfügung. Die technischen Kommunikationsstrukturen der Landesregierung zu den Behörden und Krisenstäben im Sinne einer IT-Notfallplanung ist damit gegeben.

Sehr geehrte Damen und Herren, im Landesbetrieb Daten und Information haben wir darüber hinaus ein Computer Emergency Response Team (CERT-rlp) für die Landesverwaltung von Rheinland-Pfalz eingerichtet. Diese zentrale organisatorische und technische Anlaufstelle wirkt nicht nur präventiv und reagierend, sondern trägt zur Bildung des gebotenen Sicherheitsbewusstseins bei.

Über eine rlp-Netz-weit verfügbare Informationsplattform zur IT-Sicherheit stellt das CERT-rlp regelmäßig und zeitnah Warnmeldungen über Schwachstellen in IT-Systemen bereit. Durch die enge Vernetzung durch Teilnahme an dem „Deutschen CERT-Verbund“ sowie dem in Entstehung befindlichen „Verwaltungs-CERT-Verbund (VCV)“ und der Teilnahme an der vom Bundesamt für Sicherheit in der Informationstechnik betriebenen Struktur „Allianz für Cybersicherheit“ sind eine hohe Qualität und Aktualität der bereitgestellten Information sichergestellt.

Auch im Bereich der Funkversorgung gibt es besondere Herausforderungen. So steht in

Rheinland-Pfalz und einigen anderen Bundesländern der Digitalfunk inzwischen allen Behörden und Organisationen mit Sicherheitsaufgaben zur Verfügung und wird vor allem von der Polizei bereits unter Einsatzbedingungen genutzt. In absehbarer Zeit wird er den bisherigen Analogfunk bundesweit ablösen. Die zuverlässige Verfügbarkeit ist spätestens dann für die Gewährleistung der Inneren Sicherheit unverzichtbar. Dass es sich hier um eine Kritische Infrastruktur handelt, ist offensichtlich.

Deshalb wird auch ein hoher Aufwand betrieben, um die Verfügbarkeit des Systems und seiner Komponenten sicherzustellen. Das reicht von sehr hohen Anforderungen an die Absicherung der Standorte von Basisstationen und Vermittlungsstellen über redundant ausgelegte Komponenten bis hin zu vertraglich vereinbarten sehr kurzen Reaktionszeiten des Netzbetreibers und anderer Dienstleister bei eventuellen Störungen.

Auch die Absicherung gegen Stromausfälle ist hier deutlich anspruchsvoller als noch 2011 in einem Bericht des Technik-Ausschusses des Deutschen Bundestags dargestellt. Während in diesem Bericht noch von einer batterieversorgten Überbrückung der Basisstationen von zwei Stunden die Rede war, sind die Standards hier inzwischen deutlich höher als sie es beim Analogfunk jemals waren. Die Basisstationen in Rheinland-Pfalz sind so ausgelegt, dass die batteriegestützte unterbrechungsfreie Stromversorgung für mindestens 15 Stunden ausreicht. Zusätzlich werden stationäre und mobile dieselbetriebene Netzersatzanlagen beschafft, mit denen selbst bei einem großflächigen regionalen Stromausfall das komplette Netz aufrecht erhalten werden kann. Sogar bei einem landesweiten Stromausfall könnte mit Hilfe dieser Netzersatzanlagen ein landesweites Notfallnetz aufrechterhalten werden.

Auch die betrieblichen Abläufe zur Verteilung der mobilen Netzersatzanlagen und zur Betankung bei länger andauernden Stromausfällen sind konzeptionell definiert. Ich bin deshalb sicher, dass wir beim BOS-Digitalfunk bestmöglich auf Naturkatastrophen und Angriffe auf die Netzinfrastruktur vorbereitet sind.

Trotz aller dieser Vorbereitungen müssen wir unsere Maßnahmen immer wieder evaluieren und uns dabei die Frage stellen: Haben wir alles getan, was zum Schutz der Bevölkerung erforderlich ist? Oder sind noch weitere Verbesserungen möglich?

Bund und Länder haben diese Frage im Rahmen der Entwicklung einer gemeinsamen Strategie zum Schutz Kritischer Infrastrukturen beantwortet. Sie haben dabei festgestellt, dass zum Schutz Kritischer Infrastrukturen in der Vergangenheit zwar durchaus tragfähige Konzepte entwickelt wurden, die Zusammenarbeit zwischen allen Beteiligten aber nicht immer systematisch erfolgte, sondern oftmals nur sektoral und anlassbezogen. Die Vorsorgemaßnahmen des Bundes, der Länder und Kommunen, aber auch der Wirtschaft müssen zur Gewährleistung ganzheitlicher und Ebenen übergreifender Sicherheitsstandards in Zukunft noch besser miteinander verzahnt und aufeinander abgestimmt werden.

Grundsätzlich sind jedoch die Betreiber Kritischer Infrastrukturen selbst in der Verantwortung, den notwendigen Schutz sicherzustellen.

Deshalb haben wir in Rheinland-Pfalz, ebenso wie der Bund und andere Länder, im Innenministerium eine zentrale Koordinierungsstelle zum Schutz Kritischer Infrastruk-

turen eingerichtet, bei der künftig alle Informationen gebündelt und Maßnahmen koordiniert werden. Diese Koordinierungsstelle ist nicht nur der Meldekopf für alle im Land eingehenden Informationen, sondern dient als eine Art Katalysator für die Weiterentwicklung von Schutzkonzepten.

Sie sorgt vor allem für folgende Maßnahmen:

- Bildung von institutionellen Netzwerken mit Betreibern Kritischer Infrastrukturen, Behörden und Verbänden,
- Erarbeitung und Umsetzung von Konzepten zum Schutz Kritischer Infrastrukturen,
- Sektorenübergreifende Steuerung und Bewertung von Informationen zum Schutz Kritischer Infrastrukturen auf allen Ebenen,
- Weiterleitung von Empfehlungen und Konzepten zum Schutz Kritischer Infrastrukturen an Behörden, Betriebe und an die Bevölkerung.

In einer länderübergreifenden Arbeitsgruppe „Cybersicherheit und KRITIS“ haben wir die Arbeitsschwerpunkte für die nächste Zeit festgelegt. Gemeinsam mit der Elektrizitätswirtschaft sollen eine exemplarische Bestandserhebung durchgeführt und Handlungsempfehlungen erstellt werden. Dabei werden sensible Fragestellungen gemeinsam bewertet, beispielsweise zum betrieblichen Sicherheitsmanagement, zu Maßnahmen zur koordinierten Abwehr von Angriffen oder zur Verknüpfung von betrieblichen Abwehrstrukturen mit denen der öffentlichen Verwaltung.

:

Lassen Sie mich abschließend resümieren:

Wir werden auch künftig sehr wachsam und sensibel für Anfälligkeiten und Störungen Kritischer Infrastrukturen sein müssen. Ich bin mir aber sicher, dass wir auch in diesem Bereich den Herausforderungen begegnen können, wenn alle Beteiligten bereit sind, bei ihren Sicherheitsvorkehrungen auch einmal über den Tellerrand zu blicken. Das bisherige oftmals sektorale Sicherheitsdenken muss sich zu einer neuen Risikokultur weiterentwickeln. Besonders wichtig erscheint mir dabei die partnerschaftliche und transparente Zusammenarbeit aller staatlichen und privaten Stellen, denn nur gemeinsam sind wir stark.

Gerd Gräff *ist Leitender Ministerialrat im Ministerium des Innern, für Sport und Infrastruktur Rheinland-Pfalz.*

Aus Stiftungsaktuell 52 / Juni 2013

„Neue Krisen: Ein Blick in die Zukunft“ – so der Titel der diesjährigen Konferenzreihe „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden“, die in der Landesvertretung Baden-Württemberg beim Bund in Berlin veranstaltet wurde und große Resonanz erfuhr.

Sicherheitskommunikation 2013

Der Deutsche Städte- und Gemeindebund und die Alcatel-Lucent Stiftung für Kommunikationsforschung veranstalteten am 17. Juni 2013 in Berlin die Fachkonferenz "Bürgernahe Sicherheitskommunikation für Städte und Gemeinden“. Im Fokus standen Vorträge zu Themen wie Cybersicherheit, Energiesicherheit und Schutz kritischer Infrastrukturen.

In ihrem Vortrag über die „Nationale Allianz für Cybersicherheit“ stellte *Cornelia Rogall-Grothe*, Staatssekretärin im Bundesministerium des Innern und zugleich Vorsitzende des Cyber-Sicherheitsrates, die vom Bund vorangetriebenen Schritte und Strategien im Interesse der Cybersicherheit vor. Alle Betreiber von „Kritischen Infrastrukturen“ (KRITIS) und zudem die Bevölkerung gelte es zu sensibilisieren. Als Plattform für einen Informationsaustausch wurde 2011 ein Cyberabwehrzentrum gegründet sowie ein Cybersicherheitsrat als politisches Gremium zur Festlegung der strategischen Ausrichtung. Sie appellierte, eine im März 2013 vom Kabinett verabschiedete IT-Sicherheitsrichtlinie des IT-Planungsrates auf allen Ebenen umzusetzen. Zur Unterstützung der Umsetzung sei bereits eine aus über 290 Verbänden bestehende „Nationale Allianz für Cybersicherheit“ entstanden.

Christoph Unger, Präsident des Bundesamtes für Bevölkerungsschutz und Katastro-

phenhilfe (BBK), informierte eingangs über den Stand der Krisenbewältigung bei der aktuellen Flutkatastrophe. Dass diese deutlich besser als 2002 funktioniert habe, führte er unter anderem auf Aktivitäten des Bundes zurück, der durch Ausbildung der Krisenstabsmitglieder sowie durch sein Informations- und Ressourcenmanagement Ländern und Kommunen zur Seite gestanden habe. Ferner berichtete er über die fatalen Folgen, die Extremwetterereignisse für die Sicherheit haben können, und stellte den diesbezüglichen Handlungsbedarf dar. Im Zentrum steht eine Strategie zum Schutz der KRITIS (Infos unter www.kritis.bund.de). Er stellte eine hierzu gegründete Behördenallianz vor.

Professor Wolf-Dieter Lukas, Leiter der Abteilung Schlüsseltechnologien – Forschung für Innovationen im Bundesministerium für Bildung und Forschung, berichtete von Projekten zur bürgernahen Sicherheitskommunikation im Rahmen des zivilen Sicherheitsforschungsprogramms der Bundesregierung. Dabei ginge es um bessere technische Hilfsmittel bei der Krisenkommunikation (Projekt SPIDER), um intelligenten Schutz vor bzw. Umgang mit Stromausfällen (Projekt INFOSTROM) oder um Erhöhung des subjektiven Sicherheitsgefühls in den Städten (Projekt DynASS). Das Bundesministerium fördere solche Projekte mit insgesamt 55 Mio. € im Jahr.

Professor Christian Bettstetter, Universität Klagenfurt, veranschaulichte, was Drohnen in der zivilen Nutzung für die Katastrophenabwehr zu leisten vermögen. Die enormen Folgen des Ausfalls von Internet- und Mobilfunknetzen thematisierte Professor Max Mühlhäuser von der TU Darmstadt. Dabei wies er auf die zwei Seiten des Internet hin, das einerseits die Effizienz vieler Prozesse – auch mit Nutzen für den Sicherheitsbereich – stei-

Staatssekretärin Cornelia Rogall-Grothe im Gespräch mit Dr. Erich Zielinski, Direktor der Alcatel-Lucent Stiftung, und Franz-Reinhard Habbel, Sprecher des DStGB.

Prof. Dr. Wolf-Dieter-Lukas, Leiter der Abteilung Schlüsseltechnologien – Forschung für Innovationen im Bundesministerium für Bildung und Forschung

Christoph Unger, Präsident des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK)

gere und deshalb nicht mehr hinwegzudenken sei, andererseits die Abhängigkeit unserer Gesellschaft von der dauernden Funktionsfähigkeit dieses Systems zunehmend verstärke. Aufgrund der zunehmenden Vernetzung über die IKT-Anwendungen würde der Eintritt eines black-out zunehmend größere Schäden verursachen. Neben der Virenabwehr brauche man eine „zweite Verteidigungslinie“, d. h., es müssten von zentralen Internetprovidern unabhängige Strukturen in der Kommunikation ergänzend bereitgestellt werden.

Andreas Memmert, Bürgermeister der Samtgemeinde Schladen, setzte sich mit unterschiedlichen Aspekten der Energiesicherheit mit Blick auf die kommunalen Bedürfnisse auseinander. Angesichts der erlebten und noch zu erwartenden Stromausfälle müssten Energiewirtschaft und Staat mehr tun, um black-outs zu vermeiden sowie um das Krisenmanagement so gut wie möglich vorzubereiten. Nach den Strommastenzusammenbrüchen im Münsterland sei kaum etwas geschehen. Der Staat mache es sich zu einfach, wenn er die Erfüllung der Schutzpflicht gegenüber den Bürgern auf die Städte und Gemeinden übertrage, sonst jedoch kaum Hilfe hierzu anbiete. Sowohl mit Blick auf Prävention als auch mit Blick auf das Krisenmanagement würden die Kräfte vor Ort in der Regel überfordert. Zugleich stellte er einige für Gemeinden empfehlenswerte Vorsorgemaßnahmen vor, die mit einer gründlichen Risikoanalyse beginnen.

Reinhold Harnisch, Geschäftsführer des Kommunalen Rechenzentrums Minden-Ravensburg/Lippe (krz), plädierte dafür, die IKT in den Kommunen krisenfest zu machen. Der Brand in einer von 80 zentralen Telekommunikations-Vermittlungsstellen der Telekom habe nicht vorhersehbare Auswirkungen gezeigt: Für mehrere Stunden war keinerlei elektronische Kommunikation möglich, auch die Verbindung zwischen Rechenzentren war unterbrochen. Eine halbe Millionen Menschen waren betroffen, Notrufe waren nicht erreichbar, sogar das DOI-Netz war lahmgelegt, auch Geldauszahlungen an Automaten waren nicht möglich. Die Komplexität der IKT nehme täglich zu und damit auch die Auswirkungen bei Ausfällen. Welche Weichen wir heute stellen müssen, damit uns eine sichere, verfügbare IKT auch morgen gelingt, verdeutlichte er am Beispiel des Kommunalen Rechenzentrums krz: der BSI-zertifizierte kommunale IT-Dienstleister bereite sich heute schon bezüglich Datenschutz und umfassender IKT-Sicherheit auf die zukünftigen Anforderungen vor.

Albrecht Broemme, Präsident des Technischen Hilfswerkes (THW), ging der Frage nach, woran man eine Katastrophe erkenne und wie sich die Kommune darauf vorbereiten sollte. Die Katastrophenschutzbehörden der Kreise und kreisfreien Städte haben die Aufgabe, mögliche Katastrophen im Vorfeld zu erkennen und eingetretene Schadenslagen zu bekämpfen. Hierfür sei eine umfassende Planung und Vorbereitung zwingend geboten. Die Lage in einer „echten“ Katastrophe sei meistens dadurch gekennzeichnet, dass es hierfür keine genauen Planungen gibt. Dann müssen optimal geschulte und besetzte Krisenstäbe die bestmögliche Lösung finden und umsetzen. Unterstützt würden die Katastrophenschutzbehörden im Rahmen der Amtshilfe seit Jahren erfolgreich auch durch das THW. Die Selbsthilfefähigkeit der Gesellschaft bleibe von grundlegender Bedeutung und helfe im Schadensfall, den Einsatzkräften und Institutionen zur Bekämpfung der eigentlichen Katastrophe „den Rücken frei zu halten“, so der THW-Präsident. Wichtig sei

ebenfalls, diejenigen zu kennen, mit denen man im Katastrophenfall zusammenarbeitet. Man dürfe „die Visitenkarten nicht erst auf dem Trümmerkegel austauschen".

Rolf Krost, Präsident der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, stellte in seinem Vortrag über „Infrastrukturen für Kritische Kommunikation" den Sachstand beim Aufbau des BOS-Digitalfunks dar. Die aktuelle Funkversorgung sei jetzt zu 80% erreicht und würde Ende 2014 bundesweit flächendeckend erfolgen können. Die registrierten Funkteilnehmer bezifferte er mit ca. 330.000, wobei letztlich mit ca. 500.000 Teilnehmern gerechnet werde. Im Einsatz bei der Flut habe es keine Ausfälle gegeben. Zum Thema der Objektversorgung stellte er den gegenwärtigen Stand dar: 50 Projekte auf Bundes-, 46 Projekte auf Landesebene sowie 126 Projekte durch Dritte wie ÖPNV, Flugplätze, DB-Tunnel, Einkaufszentren, Hotels und Verwaltungszentren. BDBOS-Präsident Krost wünschte sich, dass die digitale Funktechnik zunehmend von Kommunen eingesetzt werde.

Gerd Gräff, Abteilungsleiter für Katastrophenschutz und Krisenmanagement im Ministerium des Innern, für Sport und Infrastruktur Reinland-Pfalz, informierte über die strategische Ausrichtung der in Mainz eingerichteten Zentralen Koordinierungsstelle zum Schutz Kritischer Infrastrukturen. Abstimmungsrunden mit allen Energieversorgungsunternehmen hätten zu hilfreichen Standards für den KRITIS-Schutz geführt, etwa zu vereinheitlichten Meldewegen, zum Management von IT-Sicherheitsvorfällen und zu Checklisten für Kommunen für Ersatzmaßnahmen bei Stromausfällen. Das Land Reinland-Pfalz habe damit zugleich der in der „Nationalen KRITIS-Strategie" ausgesprochenen Bitte des Bundes entsprochen. Er empfahl anderen Ländern, in den Ebenen übergreifenden Austausch auch private Partner einzubeziehen und letztlich auf eine „ganzheitliche Risikokultur" hinzuwirken.

In einem anschließenden Expertengespräch wurden die Fragen zu einer gemeinsamen Bewältigung von Krisen noch einmal aufgegriffen und vertieft. Dabei wurden unter Moderation von DStGB-Sprecher Franz-*Reinhard Habbel* auch Fragen zur Besuchersicherheit bei Veranstaltungen thematisiert. Dabei legte *Christian A. Buschhoff*, (XEMP-Verlag und DStGB-Partner bei der DStGB-Dokumentation 115 „Besuchersicherheit") seine Vorstellung von einer „Kultur der Verantwortung" bei der Genehmigung von Veranstaltungen dar. Mehrere Podiumsdiskutanten begrüßten das KatWarn-System als eine gute Möglichkeit zur Warnung der Bevölkerung, an der Bürgerinnen und Bürger auf leichtem Wege partizipieren könnten. Insgesamt komme es im Krisenfall darauf an, viele Leute vor Ort persönlich zu kennen und gemeinsam nach Lösungen zu suchen. Unbedingt sollte man seine Einsatzpläne nicht nur elektronisch, sondern auch in Papierform vorhalten.

Weitere Beiträge zur Fachkonferenz sind abrufbar über www.stiftungaktuell.de.

Alcatel-Lucent Stiftung

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine gemeinnützige Förderstiftung für Wissenschaft insbesondere auf allen Themengebieten einer „Informationsgesellschaft“, neben allen Aspekten der neuen breitbandigen Medien speziell der Mensch-Technik-Interaktion, des E-Government, dem Medien- und Informationsrecht, dem Datenschutz, der Datensicherheit, der Sicherheits-kommunikation sowie der Mobilitätskommunikation. Alle mitwirkenden Disziplinen sind angesprochen, von Naturwissenschaft und Technik über die Ökonomie bis hin zur Technikphilosophie.

Die Stiftung vergibt jährlich den interdisziplinären „Forschungspreis Technische Kommunikation“, Dissertationsauszeichnungen für WirtschaftswissenschaftlerInnen sowie Sonderauszeichnungen für herausragende wissenschaftliche Leistungen.

Die 1979 eingerichtete gemeinnützige Stiftung unterstützt mit Veranstaltungen, Publikationen und Expertisen ein eng mit der Praxis verbundenes pluridisziplinäres wissenschaftliches Netzwerk, in dem wichtige Fragestellungen der Informations- und Wissensgesellschaft frühzeitig aufgenommen und behandelt werden.

www.stiftungaktuell.de

Kontakt

Alcatel-Lucent Stiftung
Lorenzstraße 10, 70435 Stuttgart
Telefon 0711-821-45002
Telefax 0711-821-42253
E-Mail office@stiftungaktuell.de
URL: http://www.stiftungaktuell.de