DStGB-Sicherheitskonferenz „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden“

Am 18. Juni 2015 veranstaltete der DStGB in Berlin die Fachkonferenz „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden“. Hauptthemen dieser inzwischen 15. DStGB-Sicherheitskonferenz waren IT-Sicherheit, Sicherheitsanforderungen an Kommunen unter dem Gesichtspunkt des Bevölkerungsschutzes sowie der Umgang mit der gestiegenen Wohnungseinbruchskriminalität.

Zum Themenbereich IT-Sicherheit wies eingangs DStGB-Sprecher Franz-Reinhard Habbel auf die jüngsten Cyberattacken wie zum Beispiel gegen den Deutschen Bundestag hin und wertete dies als zunehmende Gefahr, die sich nicht nur gegen einzelne Ausspähungsopfer, sondern gegen unser demokratisches System insgesamt richte. Neben den Verwaltungen von Bund und Ländern könne dies auch die der Kommunen jederzeit treffen. So müssten Städte und Gemeinden mehr in IT- Sicherheit investieren. Hierzu hätten die kommunalen Spitzenverbände zusammen mit vitako eine Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen erarbeitet. Diese Ausgestaltung sollte vor Ort von der Verwaltungsspitze initiiert und vorangebracht werden. Kommunale Selbstverwaltung bedeute eben auch „kommunale Selbstverantwortung“.

Martin Schallbruch, IT-Direktor im Bundesministerium des Innern, nahm zur Frage der Umsetzung des IT-Sicherheitsgesetzes Stellung. Der Gesetzgeber schreibt Betreibern Kritischer Infrastrukturen wie zum Beispiel Energieunternehmen, Banken, Wasserversorgern und Krankenhäusern vor, einen Mindeststandard an IT-Sicherheit einzuhalten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Zwar wird es beim BSI einen Kompetenzzuwachs geben, dennoch werden aber auch die Verbände der Betreiber intensiv in den Prozess einbezogen, der mittels Rechtsverordnungen zur Konkretisierung von Rechten und Pflichten des IT-Sicherheitsgesetzes führen wird.

Eine Handreichung zur IT-Sicherheit in Kommunalverwaltungen stellte Frau Dr. Marianne Wulff, Geschäftsführerin der Bundes- Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V, (VITAKO), vor. Die Handreichung diene der Ausgestaltung der Informationssicherheitsleitlinie in den Kommunalverwaltungen, die flächendeckend in Angriff genommen werden müsse, um Tendenzen einer „digitalen Sorglosigkeit“ bereits im Ansatz zu begegnen. Aufgezeigt werden Wege zum Aufbau und Betrieb kommunaler Informationssicherheits-Managementsysteme, die sich an den in Deutschland verbreiteten Standards zur Informationssicherheit orientieren sowie spezifische Bedingungen kommunaler Praxis berücksichtigen. Der Text wurde im Rahmen des Forums der IT-

Sicherheitsbeauftragten von Ländern und Kommunen von kommunalen Praktikern erarbeitet und in einer gemeinsamen Unterarbeitsgruppe der AG Cybersicherheit der Innenministerkonferenz und AG der InfoSic des IT-Planungsrates abgestimmt. Er steht im Netz unter anderem unter www.dstgb.de (Suchwort: vitako) zum kostenlosen Download zur Verfügung.

Michael Küest von der Berliner M&H IT-Security GmbH stellte unter der Überschrift “Verlässlicher Informationsschutz mittels einer innovativen Dokumentenklassifizierung – Die smarte Lösung für das e-government” Praxisempfehlungen organisatorischer und technischer Art vor, die dem Schutz vor dem zunehmenden „Datenklau“ dienen.

Unter www.m-und-h.de/novapath werden hierzu Hilfestellungen angeboten. Ergänzt wurde der Vortrag durch Ausführungen von Herrn Jan von Lüptow von der Bundesdruckerei GmbH in Berlin. Auch dort besteht ein sehr hoher Kenntnisstand im Bereich von IT-Schutztechniken wie zum Beispiel der Verschlüsselung sensibler Daten.

Dr. Stephan Klein von der Governikus GmbH berichtete unter dem Titel “Kommunaler Cyberraum” darüber, dass der IT-Planungsrat auch praxisorientierte IT-Anwendungen initiiert habe, die zu Neuentwicklungen seitens der Governikus GmbH geführt hätten. Auf der Suche nach technisch-juristisch klug durchdachten Lösungen für zentrale Aufgaben im E-Government habe man so zur sicheren Datenübertragung die Ende-zu-Ende-(OSCI-)Verschlüsselung erfunden , die beweiswertige e-Akten-Führung sowie die Langzeitarchivierung vorangetrieben und stelle nun eine Bürger-APP für den neuen Personalausweis vor, die es ermögliche, Smartphones mit NFC-Antenne als Lesegerät einzusetzen und somit die im e-government bislang nötigen Kartenlesegeräte zu ersetzen.

Dr. rer. nat. Ulrich Meissen vom Fraunhofer-Institut für offene Kommunikationssysteme und Norbert Stühmer von der Firma Bosch trugen zum Thema “Bürgernahe Sicherheit – Konzepte für vernetzte Gebäudesicherheit” vor. So werde das bekannte Warnsystem KATWARN derzeit weiterentwickelt für weitere Nutzungen, sei es für moderne Sirenen mit Sprachausgabe oder die Anbindung von Gebäudesteuerungssystemen. In Pilotprojekten wurde zum Beispiel das automatische Öffnen und Schließen von Schleusen bei Extremniederschlägen getestet. Ein Einsatz in öffentlichen Gebäuden wie zum Beispiel Schulen, um Türen und Fenster automatisch zu öffnen oder zu schließen, sei ebenso denkbar wie das nach Warnauslösung automatische Abstellen der Klimaanlage. KATWARN wurde 2013 als ein „Ausgezeichneter Ort im Land der Ideen“ geehrt, ein Preis der durch die Bundesregierung und den Bundesverband der Deutschen Industrie initiiert wurde.

Im Forum „Sicherheitsanforderungen an Kommunen“ berichtete Andreas Küspert, Kreisbrandmeister im Landkreis Garmisch-Partenkirchen, über die besonderen Anstrengungen im Interesse der Sicherheit für den G7-Gipfel auf Schloss Elmau im Juni 2015. Er beschrieb die Rolle der Feuerwehr in dem von politischen Vorgaben und den Polizeieinheiten von Bund und Ländern dominierten Sicherheitskonzept. Zu dem zeigte er die hohen Organisations- und Logistikbemühungen auf, die unternommen wurden, um die weit über 20.000 polizeilichen und nicht-polizeilichen Einsatzkräfte auf alle Eventualitäten vorzubereiten und mit allem Nötigen zu versorgen.

Frau Heike Rode vom Ordnungsamt Stadtroda stellte anschaulich die Erfahrungen einer betroffenen Stadt bei der Hochwasserkatastrophe 2013 dar. Praktisch ohne Hilfe des Landratsamtes mussten die Verantwortlichen im kreisangehörigen Stadtroda unter Bedingungen knappster Personal- und Technikressourcen ein bislang nie geübtes Krisenmanagement auf die Beine stellen, was nur mit guten Verbindungen zu privaten Akteuren vor Ort und mit dem Einsatz privater Kommunikationstechnik sowie einer ruhigen und die Menschen vor Ort mitnehmenden Krisenkommunikation gelang. Frau Rode appellierte an Städte und Gemeinden, sich im Vorfeld solcher Ereignisse gut mit Notfallplänen, Adressen und vorgehaltenen Utensilien auf das Krisenmanagement vorzubereiten. Seitens des DStGB wurde auf die Hilfestellungen hierzu in der DStGB-Dokumentation 123 „Bevölkerungsschutz in Städten und Gemeinden“ hingewiesen, die allen Kongressteilnehmern zur Mitnahme bereit lag.

David von der Lieth, stellvertretender Abteilungsleiter Gefahrenabwehr und Rettungsdienst, Feuerwehr, Bevölkerungsschutz der Stadt Düsseldorf, berichtete über die komplexe Organisation bei der Zusammenarbeit in Ad-hoc-Netzwerken beim Sturmtief ELA im Juni 2014. Die Stadt Düsseldorf war von einem extremen Sturm

betroffen und benötigte Hilfe von Einsatzkräften aus weiten Teilen des Landes. Obwohl die Großstadt organisatorisch und technisch hervorragend aufgestellt war, kam sie angesichts von 8.000 sturmbedingten Einsätzen sowie zeitweilig pro Stunde bis zu 1.200 eingehenden Notrufen an die Grenzen ihrer Kapazitäten. Als wichtigen Erfolgsfaktor für die anvisierte Resilienz sämtlicher Systeme wertete er, dass die Krisenkommunikation mit vielerlei Hinweisen frühzeitig alle beteiligten Akteure über alle für sie relevanten Entwicklungen informiert. So hätten auch die Helfer von auswärts gut orientiert und gut versorgt wichtige Hilfestellungen einbringen können.

Michael Silvan, Principal Consultant, TÜV Rheinland i-sec GmbH, berichtete, wie ein gut strukturiertes IT-Notfallmanagement eine effektive Unterstützung für das Notfall- und Krisenmanagement darstellen könne. Zunächst sei ein Risikomanagement wichtig, um die unterschiedliche Verwundbarkeit der Elemente der eigenen Organisation, und damit die nötige Priorisierung für die Notfallplanung aufzuzeigen. Bei der Notfallplanung selbst gehe es dann unter anderem darum, redundante Verfahren für die wichtigsten Geschäftsprozesse zu entwickeln, für die IT-Sicherheit optimaler Weise mit einem zweiten Rechenzentrum. Damit das toolgestützte IT-Notfallmanagementsystem im Ernstfall auch funktioniert, müsse dessen Einsatz im Vorfeld hinreichend getestet werden.

In der abschließenden Plenumsdiskussion wurde das Thema „Einbruchswelle in Deutschland: Kommunen sorgen für mehr Sicherheit ihrer Bevölkerung“ aus verschiedenen Blickwinkeln beleuchtet und diskutiert. Frau Kerstin Philipp, stellvertretende Bundesvorsitzende bei der Gewerkschaft der Polizei, und Dr. Berthold Stoppelkamp, Bundesverband der Sicherheitswirtschaft BDSW, traten dafür ein, dass die Bevölkerung besser für die Mithilfe bei der Bekämpfung von Einbruchsdelikten sensibilisiert wird. Nach dem Motto „Augen auf für Nebenan“ müssten ungewöhnliche Vorkommnisse so früh gemeldet werden, dass die Verfolgung der Täter noch chancenreich ist. Die Sensibilisierung können gut die polizeilichen Beratungsstellen voranbringen, wobei im Bereich der technischen Lösungen zur Einbruchsprävention auch das private Sicherheitsgewerbe eine gute Anlaufstelle sei. Allerdings nütze die beste Alarmtechnik wenig, wenn vor allem in ländlichen Gebieten die Polizeikräfte weit weg sind. Die Gewerkschaft der Polizei mahnt daher die Länder, die Polizeipräsenz nicht weiter durch Polizeireformen zu schmälern. Der Bundesverband der Sicherheitswirtschaft weist darauf hin, dass es in der privaten Sicherheitswirtschaft gut ausgebildete Kräfte gebe, die per Vertrag zur Sicherung von Objekten gewonnen werden können. Insgesamt müsse allerdings die Qualität im Sicherheitsgewerbe auf hohem Niveau flächendeckend durch entsprechende Vorgaben sichergestellt werden, woran es derzeit noch fehle.

(DStGB Ulrich Mohn, 22.06.2015)