ABTEILUNG IX

Aufgabenbereiche:

Mitbestimmung
PHPR Vorsitzende
Verwaltungsmodernisierung
BFA Polizeiverwaltung
Informations- und Kommunikationstechnik in der Polizei
PC-Anwenderservice GdP
Dokumentationsstelle
Bundesfinanzpolizei

1. IuK-Technik

1.1 Digitalfunk

Sachstand März 2010

Erneuter Verzug beim Aufbau des Digitalfunknetzes

„Startschuss für den Aufbau des Digitalfunk BOS" – so die verheißungsvolle Botschaft vor gut drei Jahren, als die Staatssekretäre der Innenministerien des Bundes und der Länder beschlossen hatten, noch im selben Jahr mit dem Aufbau des Digitalfunks für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) zu beginnen. Die Bundesanstalt für den Digitalfunk sollte die Koordinierung des Gesamtprojekts übernehmen.

Ein Jahr später berichtete u. a. Frontal 21 unter dem Titel „zu teuer, zu spät, zu schlecht" von schweren Mängeln beim Versuch der Einführung.

Und: Bis heute gibt es keinen flächendeckenden BOS-Digitalfunk in Deutschland – aber neue Kostenkalkulationen.

Es ist fast 20 Jahre her, dass sich die Bundesrepublik Deutschland in Art. 44 des Schengener Übereinkommens vom 19. Juni 1990 u. a. verpflichtet hat, die Möglichkeit zu prüfen, mit der Errichtung eines europaweit einheitlichen Sprech- und Datenfunksystems für Sicherheitsbehörden einen Ausgleich für den Wegfall der Grenzkontrollen zu schaffen.

Die Zeitschiene

1996, also sechs Jahre später, hat sich die Innenministerkonferenz auf die Entwicklung von Konzepten zur Einführung eines gemeinsamen digitalen Funksystems für die Sicherheitsbehörden in Deutschland verständigt.

Im Juni 2001 begann im Raum Aachen das Pilotprojekt Digitalfunk, das nach einer zweijährigen erfolgreichen Testphase mit Ablauf des Monats Juni 2003 endete.

Zur Fußballweltmeisterschaft 2006 sollten dann alle Sicherheitsbehörden und Rettungsdienste in Deutschland mit einem bundesweit einheitlichen digitalen Funksystem ausgestattet sein.

Doch weit gefehlt: Zur Fußballweltmeisterschaft 2006 mussten Behörden und Organisationen mit Sicherheitsaufgaben (BOS) ohne den angedachten flächendeckenden Digitalfunk auskommen. Eine Ursache lag im Streit der Haushälter über die Notwendigkeit und die Verteilung der Kosten zwischen Bund und Ländern.

Im Februar 2005 legte der damalige Bundesinnenminister Otto Schily den Innenministern und -senatoren der Länder eine Fortschreibung des Konzeptes zum Aufbau und Betrieb des Digitalfunks für die BOS vor. Es sah die Errichtung und den Betrieb eines Rumpfnetzes durch den Bund und die Erweiterung durch die Länder vor. Die Innenministerkonferenz beschloss daraufhin, das Gesamtnetz bis spätestens Ende 2010 in Betrieb zu nehmen. Doch bislang wurde immer wieder von zeitlichen Verzögerungen berichtet, was von den verantwortlichen Stellen zwar reflexartig dementiert wurde, aber dennoch erfüllten sich die Negativ-Prophezeiungen regelmäßig.

Starke Skepsis ist auch gegenüber der aktuellen Planung angebracht. Denn zwischenzeitlich wurde eingeräumt, dass es für topografisch schwierige Gebiete bis Ende 2010 möglicherweise noch keine Funkabdeckung geben werde. Gemeint sind damit allerdings auch Gebiete, wo es noch keine Funkmasten gibt. Die Verantwortlichkeit für die Ertüchtigung der Funkstandorte liegt für das Kernnetz beim Bund, ansonsten bei den Ländern.

Am 01. April 2009 beschloss der Verwaltungsrat der BDBOS, die Fertigstellung des digitalen Netzes bis Ende 2012 zu strecken.

Als Begründung für die neue Zeitrechnung:

Es würden mehr Basisstationen, als ursprünglich geplant, benötigt. Auch die Beschaffung und/oder Ertüchtigung der Funkstandorte gestalte sich erheblich schwieriger, als ursprünglich angenommen. Dennoch erhielt inzwischen die französische Firma Alcatel-Lucent den Zuschlag für ihr verbindliches Angebot für den Regelnetzbetrieb.

Die Kosten

Nun wurde bekannt, dass es nicht nur zeitliche Verzögerungen bei diesem Großprojekt gibt, sondern dass auch die Kosten explodieren. Zunächst war der Anteil des Bundes von 2,6 auf 3,6 Milliarden Euro angestiegen.

Zuletzt hatte die BDBOS eine Kostenschätzung von 4,5 Milliarden Euro veranschlagt.

WELT ONLINE berichtet am 25. Februar 2010 über den Wortlaut eines dort vorliegenden Sachstandsberichtes aus dem Bundesinnenministerium, in dem nun von 10 Milliarden Euro die Rede ist. Zuletzt hatte sich der Haushaltsausschuss des Deutschen Bundestages mit der Frage befasst, wie teuer das digitale Funknetz nun tatsächlich wird. Einige offene Fragen

über die Gesamtkosten führten u. a. dazu, dass der Ausschuss bereits im Mai 2009 eine Sperrung der Mittel verfügt und die Freigabe der nötigen Mittel für den Regelbetrieb des Netzes am 25. Februar 2010 nicht beschlossen hatte. Der Tagesordnungspunkt wurde abgesetzt und auf den 03. März 2010 vertagt.

Es handelt sich hierbei um die Freigabe von rund 500 Millionen Euro für den Regelbetrieb des Netzes. Die Sitzung des Haushaltausschusses war nicht öffentlich. Bekannt wurde jedoch, dass er die Mittelsperre teilweise aufgehoben und damit 340 Millionen Euro für den Regelbetrieb freigegeben hat.

Nach alledem gehen die Verantwortlichen nun davon aus, dass sich die flächendeckende Inbetriebnahme des Digitalfunknetzes bis Ende 2013 verschieben wird. Der Herausgeber der NET (Zeitschrift für Kommunikationsmanagement), Frank Bakasch, hat in Ausgabe 5/09 ausgeführt:

> „Bis Ende März 2009 war nach Angaben der BDBOS die Systemtechnik an ca. 200 Basisstationen installiert, davon befanden sich 133 in Betrieb … Wir erinnern uns: Ende Oktober 2008 gab es 90 Funkstandorte mit Inbetriebnahme … D. h. in fünf Monaten sind 43 dazugekommen, 8,6 pro Monat. Ist das noch Roll-out? Denn gebraucht werden mindestens 4.000. Ginge es so weiter, wäre das Netz also – rein rechnerisch – in 37 Jahren fertig."

Bleibt zu hoffen, dass dieses Rechenexempel nicht Realität wird, zumal jede weitere Verzögerung mit erheblichen zusätzlichen Kosten verbunden ist.

DB Telematik scheidet für den Aufbau und Betrieb des Netzes aus

Am 27. Oktober 2006 behandelte der Deutschen Bundestag einen Antrag der FDP-Fraktion.

Mit diesem Antrag wurde die Bundesregierung aufgefordert:

> BOS-Digitalfunk neu ausschreiben – Neustart mit transparenter Auftragsvergabe unter Berücksichtigung des Wirtschaftlichkeitsgrundsatzes

Begründet wurde der Antrag damit, dass die DB Telematik am 31. Juli 2006 ein Angebot in Höhe von 2,6 Milliarden Euro vorgelegt hatte, der im Haushalts- und Finanzplan für den Bund veranschlagte Kostenrahmen jedoch nur 1,1 Milliarden Euro betrug.

Die FDP forderte, die Verhandlungen über den Betrieb des BOS-Digitalfunks mit der DB Telematik sofort zu stoppen und den Betrieb des Digitalfunksystems neu auszuschreiben und mit einem transparenten Auftragsvergabeverfahren schnellstmöglich zu realisieren. Zusätzlich sollte die Errichtung der Bundesanstalt bis zum Abschluss des neuen Vergabeverfahrens ausgesetzt werden.

Begründet wurde der Antrag damit, dass eine neue Ausschreibung nicht nur die Kosten für den Digitalfunk reduzieren, sondern die technische Verlässlichkeit und die baldige Einführung sicherstellen, gegebenenfalls sogar beschleunigen würde.

Von der CDU/CSU-Fraktion wurde entgegnet, dass keine der Forderungen der FDP gerechtfertigt sei. Es sei bekannt, dass die Entscheidung, den Aufbau und Betrieb des Digitalfunknetzes an die Bahntochter DB Telematik zu vergeben, aufgrund der besonderen Sicherheitsbedürfnisse gerechtfertigt war und ist.

Alles deute darauf hin, dass die Verhandlungen mit der DB Telematik innerhalb des vorgesehenen Zeitrahmens bis zum 15. Dezember 2006 erfolgreich abgeschlossen werden.

Die derzeitigen Verhandlungen zwischen der Bundesregierung und der DB Telematik seien in einer sehr schwierigen Phase. Lange Zeit habe es so ausgesehen, als würde sich die DB Telematik an die Preisvorgaben halten. Kurz vor Vertragsunterzeichnung habe man offensichtlich noch einmal nachkalkuliert und plötzlich festgestellt, dass der unternehmerische Gewinn, der so verlockend erschien, auch ein unternehmerisches Risiko mit sich bringt. Schließlich handele es sich um eine sicherheitsrelevante Infrastruktur. Dieses unternehmerische Risiko sollte dann über exorbitante Risikozuschläge auf den Auftraggeber abgewälzt werden.

Auf der Grundlage eines angepassten Angebots verhandelt der Bund mit der DB Telematik weiter. Der neue Vorschlag der DB Telematik, mit den Synergie-Effekten eines starken Partners (T-Systems) innerhalb des vorgegebenen Finanzrahmens das Projekt realisieren zu können, sei prüfenswert. Allerdings sei auch klar, dass es dabei keine Abstriche bei der Qualität, bei der Verfügbarkeit sowie bei der Sicherheit des Funks geben darf.

Es sei auch richtig, dass der Bund parallel zu den weiteren Verhandlungen Alternativmodelle entwickeln würde, um für den Fall der Fälle auf eine weitere Option zurückgreifen zu können. Dies werde auch von den Ländern ausdrücklich so gesehen. Man wolle sich parallel zur Vergabe des Betriebs die Alternative des Eigenbetriebs als Möglichkeit offenhalten. Bund und Länder müssten jetzt alles daransetzen, dass die Verhandlungen im Dezember 2006 erfolgreich zu Ende gebracht werden.

Am 30. November 2006 hatte die DB Telematik ihr abschließendes Angebot für Aufbau und Betrieb des Systems vorgelegt. Für einen Zeitraum von 15 Jahren wurden Kosten in Höhe von 5,7 Milliarden Euro veranschlagt. In diesen Gesamtkosten sind ein Risikozuschlag und ein Aufschlag für Inflationseffekte in Höhe von 600.000 Euro enthalten. Abgesichert werden sollen damit Unabwägbarkeiten, die nicht mit der von der DB Telematik zu verantwortenden Technik einhergehen könnten. Dieses Angebot war bis Ende März 2007 gültig. Es war Anfang Dezember 2006 Gegenstand einer Telefonkonferenz der Innenstaatssekretäre.

Schnell war man sich zwischen Bund und Ländern offensichtlich einig: Das Ganze ist zu teuer.

Außerdem würden die Leistungsmerkmale deutlich hinter den Anforderungen an das Netz zurückbleiben. Zwischen Bundesinnenminister Schäuble und Bahnchef Mehdorn gab es daraufhin ein weiteres Krisengespräch. Im Bundesinnenministerium dachte man zwischenzeitlich über Alternativen nach. Geredet wurde schon seit längerer Zeit von einem Plan „B".

Eine der Alternativen war eine neue Ausschreibung, mit der Folge, dass eine weitere Verschiebung des Projektes zu erwarten war. Das wollte man im Bundesinnenministerium unbedingt vermeiden. Eine weitere Alternative: Beschaffung, Installation und Betrieb des Netzes sollen neu aufgeteilt werden. Hiervon könnte die EADS, die schon die Ausschreibung für die Netzwerktechnik gewonnen hat, profitieren. Auch die T-Systems, die zwar als Subunternehmer bei der

DB Telematik gehandelt wurde, war laut Insiderinformation als Netzbetreiber denkbar. Denkbar war aber auch, der neu gegründeten Bundesanstalt (BDBOS) den Netzbetrieb zu übertragen.

Am 13. Dezember 2006 beriet der Lenkungsausschuss abschließend über das Angebot der DB Telematik und beschloss, deren Angebot abzulehnen.

Vodafone stellt die technischen und finanziellen Eckpunkte ihres Angebotes dar

Repräsentanten der Vodafone GmbH führten im Februar 2007 ein Gespräch mit der GdP, in dem sie ihr Konzept für einen digitalen Polizeifunk vorgestellt haben. Mit diesem Konzept sollten ein hoher technischer Standard, die Zuverlässigkeit in der Nutzung und die absolute Wirtschaftlichkeit sichergestellt werden.

Bereits im September 2006 habe man bei der ersten Hockey-WM der Herren in Deutschland mit der Bereitstellung des Vodafone-ProfiFunk sichergestellt, dass die Abstimmung zwischen den Organisatoren sowie den Sicherheits- und Rettungskräften während des internationalen Sportereignisses reibungslos funktionierte.

Die Organisatoren, der Fahrdienst und die Sicherheitskräfte (Polizei, Feuerwehr und DRK) haben schnell, effizient und vor allem sicher über die neue Profifunk-Lösung kommuniziert.

Da an dem Ziel der Einführung des digitalen Funksystems bis 2010 auch nach Scheitern der Verhandlungen mit der DB Telematik festgehalten werde, stellte Vodafone die technischen wie finanziellen Eckpunkte ihres Angebotes vor. Demnach sollte bereits im Jahr 2007 die Möglichkeit bestehen, über ein modernes, leistungsfähiges und den Anforderungen der Inneren Sicherheit entsprechendes digitales Polizeifunksystem zu verfügen.

Konkret sieht das Vodafone-Angebot so aus:

- Vodafone bietet den deutschen BOS die Mitnutzung des bestehenden GSM-Netzes mit 20.000 Standorten und 50.000 Funkzellen an. Damit entfiele der zeitintensive Aufbau eines eigenständigen Tetra-Netzes, das ohnehin nie eine vergleichbare Netzabdeckung, Gebäudeversorgung und Datendienste wie das Vodafone-Netz bieten kann.
- Aus finanzieller Sicht stellte sich das Vodafone-Angebot wie folgt dar:
  - 35 Euro (zzgl. USt) pro Nutzer pro Monat mit unbegrenzter Sprachtelefonie im BOS-Netz
  - Bei 260.000 Nutzern (entspricht allen Polizisten) ergibt sich ein Gesamtaufwand von 0,9 Mrd. Euro für 10 Jahre (Annahme: alle Nutzer migrieren bis 2010).

Dieses entspricht einer heutigen Einmalzahlung von 0,56 Mrd. Euro (bei angenommenen Kapitalkosten von 7 %).

- GSM ist der Mobilfunkstandard in Europa. Eine Anbindung eigenständiger Tetra- und Tetrapol-Netze der Nachbarländer ist technisch machbar. Vodafone kann also kurzfristig den Bund unterstützen und dabei gleichzeitig den Weg für eine europakompatible Lösung offen halten.
- Vodafone bietet an, dass zentrale Netzkomponenten – wie Teilnehmerdatenbank und Vermittlungstechnik – in einer BOS-Betreibergesellschaft zusammengefasst werden, die von den BOS geführt und kontrolliert werden kann.
- Vodafone hat in Deutschland 30 Millionen Kunden. Nach Anpassung bezüglich Funktionalität, Kapazität und Betriebssicherheit kann Vodafone mit Unterstützung der Partner Siemens, Ericsson und IBM die Anforderungen der BOS erfüllen und teilweise übertreffen. Dank der höheren Übertragungsgeschwindigkeit sind mit dem Vodafone-Netz moderne Datendienste, wie Übertragung von Bildern und Bewegt-Bildern sowie Datenabfragen, erst möglich.
- Bei Großschadensfällen kann Vodafone die Netzkapazitäten durch Halfrate- Modus ausweiten, Gebiete durch überlappende Zellen versorgen und mobile Basisstationen einsetzen. Die BOS-Nutzer erhielten zusätzlich eine Priorisierung, so dass den 260.000 Polizisten im Extremfall ein Netz, das für 30 Millionen Nutzer – d. h. das Hundertfache – ausgelegt ist, zur Verfügung stünde.
- Bei zeitnaher Beauftragung kann Vodafone Profifunk BOS ab Herbst 2007 anbieten, sowohl bundesweit als auch für einzelne Bundesländer.
- Vodafone möchte weiterhin die BOS bei der Migration auf digitale Sprach- und Datenkommunikation unterstützen. So ist Vodafone bereit, z. B. über die Zusammenschaltung mit einem Tetra-Netz sowie über Datenlösungen für die BOS zu reden.

Bewertung:

Das von Vodafone vorgestellte Angebot hatte dem Beschaffungsamt des BMI bereits im Dezember 2005 vorgelegen. Inhaltlich, kostenmäßig und technisch gibt es keinen Unterschied zu dem neuen Angebot.

Digitalfunknetz im Juni 2007 für die Einsatzkräfte beim G-8-Gipfel

Das Land Mecklenburg-Vorpommern hat den Auftrag zum Aufbau und Betrieb eines digitalen Funknetzes für die Einsatzkräfte beim G-8-Gipfel an Motorola vergeben.

Ausgeschrieben worden war ein temporäres Digitalfunknetz in der Region um Heiligendamm, wo der G-8-Gipfel im Juni d. J. stattfinden wird.

EADS und T-Systems haben sich für diesen Auftrag n i c h t beworben.

Das Land hatte dem Bund vorgeschlagen, sollte die EADS den temporären Aufbau und Betrieb durchführen, dieses als Teil des bundesweit geplanten Netzes zu betrachten und in Anrechnung zu bringen. Das Bundesinnenministerium soll dieses Ansinnen jedoch abgelehnt haben, da es derzeit noch keine festgelegte Netzplanung gebe und auch noch kein Netzbetreiber feststehe.

Gemäß dem Systemlieferantenvertrag für das bundesweite Digitalfunknetz muss EADS im Rahmen der Vertragserfüllung noch vier Referenznetze aufbauen (Berlin, Hamburg, Stuttgart, München). Das lokale Netz in Heiligendendamm hätte damit nicht in das Referenzkonzept gepasst.

Motorola wird nun das Digitalfunknetz in der Region Heiligendamm aufbauen, betreiben und nach dem G-8-Gipfel wieder abbauen.

Ein Betreiberkonzept für den digitalen BOS-Funk ist noch nicht erkennbar.

Es müssen noch etliche Abstimmungen zwischen dem Bund und den Ländern erfolgen, ehe das Betreiberkonzept für den bundeseinheitlichen Digitalfunk endgültig feststeht.

Der derzeitige Plan sieht einen Zwischenbetrieb durch die Telekom und einen Teilbetrieb durch den Systemlieferanten (EADS) vor.

In dem Verwaltungsabkommen zwischen Bund und Ländern ist die Möglichkeit der Beistellungen eröffnet worden, d. h., einzelne Länder können bestehende Netze oder Netzteile sowie Standorte in das Gesamtnetz einbringen. Einige Länder wollen grundsätzlich auf Beistellungen verzichten, andere hingegen nicht. Diese Beistellungen unterliegen jedoch einer Qualitätsprüfung, ob diese Netzbestandteile den Anforderungen technologisch entsprechen und im Gesamtnetz praktizierbar sind.

Die Ausschreibung und die Verträge im Zusammenhang mit dem Aufbau und Betrieb des Netzes werden nach dem BDBOS-Gesetz durch die Bundesanstalt vergeben.

Die Akquisition von Standorten und die Bereitstellung der notwendigen Übertragungswege sollen nunmehr, in Abstimmung mit der Projektorganisation, den Ländern obliegen. Nicht alle Länder verfügen aber über die personellen Ressourcen zur Erfüllung dieser Aufgaben. Sie werden externe Hilfe in Anspruch nehmen müssen, um diese zu bewältigen. Das lässt jedoch weitere Kostensteigerungen und Zeitverzögerungen erwarten.

Während EADS mit Unterstützung durch die Siemens AG als Konsortialpartner die Systeme liefern, wird die EADS dem Vernehmen nach die T-Systems mit den Aufgaben des technischen Netzwerkcontrollings beauftragen.

Dieses neue Konzept erfordert die Überarbeitung des bereits paraphierten Bund- Länder-Abkommens zur Einführung des Digitalfunks. Eine Verabschiedung des überarbeiteten Konzeptes, die für die nächste Sitzung der IMK Ende Mai 2007 vorgesehen ist, wird von Insidern in Frage gestellt.

Funkflächenversorgung durch das C-Netz der Telekom

Die Telekom besitzt 6.000 Mobilfunkstandorte, von denen 3.000 für das bereits abgeschaltete C-Netz zur Verfügung standen und nutzbar wären.

Eine Funkflächenversorgung wäre, so die Telekom, damit gesichert. Die Telekom bietet außerdem eine Lösung für die Organisation des zentralen Bereiches an, nämlich ein vorhandenes Backbone-Netz, ein Netzmanagement und die notwendige Dezentralisierung.

Zwei Management-Center sollen als Leitstellen mit einer Backup-Lösung den Betrieb des Netzes sichern.

Die Telekom könnte nicht nur für die Standorte, deren Ertüchtigung (Zugangsicherheit, Notstromversorgung und Netzanbindung) verantwortlich sein, sondern auch für die notwendigen Baugenehmigungen.

Verwaltungsabkommen zum Start des digitalen Sprech- und Datenfunksystems für alle Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Am 01. Juni 2007 unterzeichneten die Innensenatoren/Innenminister von Bund und Ländern das Verwaltungsabkommen über die Zusammenarbeit von Bund und Ländern beim Aufbau und Betrieb des Digitalfunks der BOS.

Neben der Zusammenarbeit regelt das Verwaltungsabkommen die Finanzierung des Digitalfunks und die Beteiligung der Länder an der Arbeit der Bundesanstalt für den Digitalfunk der BOS (BDBOS).

Die BDBOS hat am 02. April 2007 die Aufgabe der Einführung des Digitalfunks in Deutschland für den Bund übernommen. Mit der Unterzeichnung des Verwaltungsabkommens durch die Innenminister/Innensenatoren nimmt die BDBOS diese Aufgabe auch für die Länder wahr.

Sie fungiert damit gegenüber Unternehmen als Auftraggeberin von Bund und Ländern, ermöglicht die gemeinsame Vergabe von Aufträgen und stellt somit eine in Deutschland einzigartige Einrichtung dar, so das BMI.

Die Kosten für den Aufbau und Betrieb des digitalen Funknetzes werden durch die Innenminister auf rund 4,5 Milliarden Euro veranschlagt.

Der Auftrag für den technischen Aufbau des Netzes erging schon vor geraumer Zeit an die Firma EADS, die diesen zusammen mit Siemens betreiben wird.

Nachdem die DB Telematik mit ihrem Angebot für den Netzbetrieb gescheitert ist, werden die Firma EADS und die BDBOS bis zu einer endgültigen Auftragsvergabe den Netzbetrieb übernehmen. Eine Ausschreibung für den Netzbetrieb ist für Ende dieses Jahres vorgesehen.

Das neue digitale Netz soll nun zunächst in Niedersachsen, Hamburg, Berlin, Nordrhein-Westfalen und Bayern erprobt werden.

Sachstand der Einführung des Digitalfunks im August 2008 im Innenausschuss des Landtags NRW

Zur Sitzung des Innenausschusses im Landtag NRW am 14. August 2008 wurde folgendes Votum über den Sachstand der Einführung des Digitalfunks abgegeben (Auszug):

Sachstand:

Bis zum Jahre 2011 wird in Deutschland das einheitliche Digitalfunknetz für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) aufgebaut. Dabei werden mehrere hundert derzeit separat betriebene analoge Netze durch ein einziges ersetzt, so dass die Kommunikation deutlich effizienter und sicherer wird. Weiterhin bieten neue technische Funktionalitäten auch die Möglichkeit zur taktischen Optimierung von Einsätzen.

Das bundesweite Projekt geht aktuell von der Planungs- in die Netzaufbauphase über.

Wesentliche konzeptionelle Arbeiten sind abgeschlossen bzw. befinden sich wie geplant im Abschluss. Der so genannte Master-Roll-out-Plan sieht den Aufbau des Netzes mit circa 3.600 Basisstationen, 62 Vermittlungs- und vier Transitvermittlungsstellen bis Ende 2010 vor.

Der Bund wird dabei das so genannte Kernnetz bereitstellen, an das die Länder ihre bundesweit insgesamt 45 Netzabschnitte, die anteilig vom Bund und dem jeweiligen Land finanziert werden, anschließen. In Nordrhein-Westfalen wurden sechs Netzabschnitte festgelegt (entsprechend den fünf Regierungsbezirken, jedoch der Bezirk Düsseldorf geteilt in Bereich Düsseldorf und Essen); der finanzielle Anteil des Bundes daran beträgt gegenwärtig 47,74 %.

Bundesweiter Sachstand:

Kernnetz

Die Errichtung des Kernnetzes wurde begonnen. Ab Herbst dieses Jahres können daran betriebsbereite Basisstationen angeschlossen werden.

Endgeräte

Parallel zum Aufbau des Kernnetzes wurden Vorgaben für die Endgerätebeschaffung erarbeitet. Diese Vorgaben dienen dazu, den technisch reibungslosen Betrieb von Geräten verschiedener Hersteller sicherzustellen. Die Hersteller erhalten so die Möglichkeit, ihre Geräte rechtzeitig vor den Vergabeverfahren der Länder technisch anzupassen.

Ab Oktober 2008 können die Hersteller ihre Endgeräte zertifizieren lassen.

Betrieb

Im Rahmen des von der BDBOS durchgeführten Vergabeverfahrens über den „Betrieb des Digitalfunknetzes der BOS“ wurden Bewerber zur Einreichung vorläufiger und weiter verhandelbarer Angebote aufgefordert. Der Zuschlag soll Anfang 2009 erteilt werden. Die Übergangszeit wird von EADS als Interimbetreiber abgedeckt. In Summe sind seitens der BDBOS in den Bereichen Netzplanung, Netzaufbau und Betrieb die konzeptionellen Planungen weitgehend abgeschlossen und die erforderliche Aufstellung zum Roll-out eingerichtet.

Stand in den anderen Starterländern

Neben Nordrhein-Westfalen zählen Berlin, Hamburg, Niedersachsen, Baden-Württemberg und Bayern zum Kreis der Starterländer. Dort sind im Wesentlichen dieselben Startprobleme wie auch in Nordrhein-Westfalen aufgetreten. Es liegt auf der Hand, dass die Stadtstaaten im Vergleich zu den Flächenländern deutlich kürzere Aufbauzeiten benötigen.

Nordrhein-Westfalen hat sich dafür entschieden, den Betrieb mit zertifizierten Endgeräten aufzunehmen, um Fehlinvestitionen zu vermeiden. Auch daher wurde hier der Betriebsbeginn auf Februar 2009 festgelegt.

Bundesweite Koordination

Die Länder und der Bund werden sich ab Juli 2008 monatlich mit der BDBOS abstimmen.

Nordrhein-Westfalen hat dabei die Aufgabe übernommen, die Länderinteressen gegenüber der BDBOS zu koordinieren.

Projektrisiken

Das derzeit verwendete bundesweite analoge Funksystem der Behörden und Organisationen mit Sicherheitsaufgaben besteht aus lokalen, von unterschiedlichen Aufgabenträgern betriebenen Teilnetzen.

Ziel des Projektes ist, ein bundesweit einheitliches flächendeckendes zellulares digitales Sprach- und Datenfunknetz für alle BOS zu errichten.

Es soll die behördenübergreifende Kommunikation bei der Bewältigung der täglichen Aufgaben als auch im Krisen- und Notfalleinsatz sicherstellen und mehr als 2 Millionen Anwendern bzw. rund 500.000 Nutzern gleichzeitig zur Verfügung stehen. Damit wird es weltweit das größte Netz dieser Art sein.

Die Integration aller BOS mit einer solchen Nutzerzahl in einem digitalen Funknetz ist bisher in keinem anderen Land vergleichbarer Größe erfolgt.

Es liegt daher auf der Hand, dass ein solches Projekt in der Abwicklung Risiken –insbesondere auch bei der zeitlichen Abfolge – birgt. Die zwischen Bund und Ländern vereinbarte Arbeitsteilung erfordert wegen der wechselseitigen Abhängigkeit einen hohen Koordinierungsaufwand. Die Beteiligung aller kommunalen Aufgabenträger ist sehr zeit- und arbeitsaufwändig. Eine punktgenaue zeitliche Synchronisation aller Beteiligten mit allen ihren Aktivitäten dürfte in der Praxis kaum erreichbar sein.

Das enge Terminkorsett des so genannten bundesweiten Roll-out-Plans ist insbesondere in den Startregionen wie dem Regierungsbezirk Köln sensibel für Störungen.

Die Akquisition von Standorten für Basisstationen unterliegt neben dem Termin- auch einem zusätzlichen Kostenrisiko. Diese Risiken ergeben sich u. a. dadurch, dass die nach Funkplanung bestgeeigneten Standorte z. B. aufgrund erfolgloser Vertragsverhandlungen mit den Eigentümern, Denkmalschutzes, Sorgen Betroffener wegen ,,Elektrosmogs“ durch Alternativen ersetzt werden müssen, was zu einer Erhöhung der Anzahl der Basisstationen und damit der Errichtungskosten führt.

Die Infrastruktur des BOS-Digitalfunks ist ein Hochsicherheitsnetz, das gerade dann funktionsfähig sein muss, wenn andere Kommunikationssysteme beispielsweise wegen besonderer Naturereignisse, Anschlägen oder flächendeckend unterbrochener Stromversorgung ausgefallen sind. Die resultierenden materiellen Sicherheitsanforderungen an die Basisstationen führen zu einer großen Kostenvarianz, je nachdem, ob es sich beispielsweise um Liegenschaften der Polizei mit ohnehin vorhandenen Sicherheitsvorkehrungen oder die Errichtung neuer Sendemasten „auf der grünen Wiese“ handelt.

▸ Gesundheitliche Auswirkungen des Digitalfunks werden erforscht

Noch während der PMRExpo 2008 wurde bekannt, dass die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) und das Bundesamt für Strahlenschutz (BfS) eine Zusammenarbeit über Fragen gesundheitlicher Auswirkungen des Digitalfunks

vereinbart haben. Schwerpunkt dieser Vereinbarung ist die Durchführung von Forschungsvorhaben.

Der Präsident der BDBOS betonte: „Der Digitalfunk bietet Feuerwehren, Polizeien und Rettungskräften zahlreiche Vorteile für ihre tägliche Arbeit. Für die Bürgerrinnen und Bürger bedeutet dies eine verlässliche und noch schnellere Hilfeleistung im Notfall. Gleichwohl nehmen wir die Vorbehalte gegenüber den Wirkungen der neuen Funkgeräte und Sendestationen auf die Gesundheit ernst."

Mit den Forschungsvorhaben wollen BDBOS und BfS die noch bestehenden Unsicherheiten über die Auswirkungen der beim Digitalfunk genutzten Frequenzbereiche weiter verringern. Gegenstand der ersten beiden Studien sind mögliche Wirkungen elektromagnetischer Felder der Funkgeräte auf den menschlichen Körper.

Der Präsident des BfS sagte dazu: „Beim Aufbau des neuen Funknetzes müssen Gesundheitsvorsorge und Strahlenschutz für die Nutzerinnen und Nutzer des Digitalfunks sowie für die Bevölkerung insgesamt eine wichtige Rollen spielen."

Hierzu gehört auch eine transparente Information der Öffentlichkeit.

Andere europäische Staaten wie Großbritannien, Belgien und die Niederlande nutzen bereits seit einiger Zeit Tetra-Netze für deren Sicherheitsbehörden und begleiten die Nutzung mit Forschungsstudien.

▸ Weitere Verzögerung bei der bundesweiten Einführung des digitalen Funknetzes für die Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Um mindestens zwei Jahre, also bis Ende 2012, wird sich die bundesweite Einführung des digitalen Funknetzes für die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) verzögern.

Der Verwaltungsrat der Bundesanstalt für den Digitalfunk der BOS (BDBOS) hat das Ziel, den Aufbau eines bundesweit einheitlichen Digitalfunknetzes bis Ende 2010 abzuschließen, aufgegeben. Am 01. April 2009 (kein Aprilscherz) beschloss der Verwaltungsrat, den Roll-out bis Ende 2012 zu strecken.

Als Begründung für die neue Zeitrechnung werden die beim bisherigen Netzaufbau gesammelten Erfahrungen, dass mehr Basisstationen benötigt werden, als ursprünglich zugrunde gelegt wurde, angeführt. Auch die Beschaffung und/oder Ertüchtigung der Funkstandorte gestalte sich erheblich schwieriger, als ursprünglich angenommen.

Als Nächstes ist im laufenden Vergabeverfahren die Abgabe verbindlicher Angebote der noch im Wettbewerb stehenden Anbieter (NSN, EADS/T-Systems, Alcatel-Lucent) für den Betrieb des Netzes zum 15. Mai 2009 vorgesehen.

Anmerkung:

Der Verwaltungsrat der BDBOS überwacht die Geschäftsführung durch die Präsidentin oder den Präsidenten und unterstützt diese oder diesen bei der Erfüllung ihrer oder seiner Aufgaben.

Der Bund und jedes Land erhalten jeweils einen Sitz im Verwaltungsrat. Den Vorsitz im Verwaltungsrat hat das den Bund vertretende Mitglied. (Auszug aus § 5 BDBOS-Gesetz)

▸ EADS Secure Networks erhält den Auftrag zum Aufbau eines bundeseinheitlichen digitalen Sprech- und Datenfunksystems

Das von Motorola beantragte Nachprüfungsverfahren vor der Vergabekammer beim Bundeskartellamt ist abgeschlossen.

Motorola hatte u. a. die Nichtberücksichtigung von mehreren Tetra-Lizenzen durch die EADS gerügt (siehe DP 07/2006). Der Motorola-Antrag wurde aus verfahrensformalen Gründen abgelehnt.

Am 28. August 2006 erteilte das Beschaffungsamt des Bundesministeriums des Innern den Zuschlag im Vergabeverfahren zur Beschaffung der Systemtechnik für den BOS-Digitalfunk an die EADS Secure Networks.

Im Rahmen dieses Auftrages wird die EADS als Generalunternehmer gemeinsam mit Siemens bis zum 31. Dezember 2010 ein bundesweites Tetra-Digitalfunknetz realisieren. Insgesamt hat das Projekt für die EADS ein potenzielles Volumen von bis zu 1 Milliarde Euro.

Die Vergabeentscheidung des Bundesinnenministeriums basiert auf der Auswertung des schriftlichen Angebotes der EADS vom 06. Dezember 2005, einem umfangreichen Labortest zur Verifikation der angebotenen technischen Eigenschaften und Feldtests in Berlin und Baden-Württemberg zur Prüfung weiterer Systemfunktionen unter taktisch operativen Einsatzbedingungen. Sowohl im schriftlichen Angebot als auch in allen Testphasen konnte die EADS erfolgreich den Nachweis des wirtschaftlichsten Angebots im Wettbewerb erbringen.

Bundesinnenminister Dr. Wolfgang Schäuble betonte anlässlich der Zuschlagserteilung: „Dieses Projekt beweist einmal mehr, dass Bund und Länder erfolgreich zusammenarbeiten können. Nun werden wir zügig mit dem Aufbau des BOS-Digitalfunks beginnen."

Weitere Eckpfeiler für die Einführung des Digitalfunks sind die Errichtung einer Bundesanstalt und das Verwaltungsabkommen über die Zusammenarbeit von Bund und Ländern. Bundestag und Bundesrat haben dem Gesetz zur Errichtung der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) zugestimmt. Das Verwaltungsabkommen haben Bund und Länder im Mai paraphiert. Die Unterzeichnung durch die Minister und Senatoren des Innern ist für November dieses Jahres geplant.

Bleibt nur noch zu hoffen, dass es sich bei der Technik, die nun aufgebaut wird, um Technik von heute für morgen handelt.

Denn dieses Verfahren macht einmal mehr deutlich, dass bei derartigen IT-Großprojekten die Probleme bereits mit der Ausschreibung beginnen. So werden Pflichtenhefte und Vorgaben erstellt, die – nicht selten – mehrere Aktenordner füllen. Für die Anbieter bedeutet dies eine fast endlose Sisyphus-Arbeit.

Nach Erteilung des Zuschlags kommt meist die Ernüchterung, weil die technische Entwicklung die ursprünglichen Vorgaben in den Ausschreibungsunterlagen meist schon weit überholt hat. Für Änderungen ist dann in der Regel aus vergaberechtlichen Gründen zu spät, denn sie sind nicht erlaubt. Damit würde unterlegenen Bietern zudem die Möglichkeit zur Klage eröffnet und das Verfahren müsste neu aufgerollt werden.

Hier ist eindeutig der Gesetzgeber gefordert. Die Vergabeprozesse müssen entschlackt und flexibler gestaltet werden. In einer Zeit der schnellen Entwicklungen und Anpassungen dürfen gesetzliche Regelungen und Vorgaben nicht dazu führen, dass heute eine Technik von gestern gekauft werden muss.

1.2 Körperscanner

Verwendung von Body-Scannern bei der Luftsicherheitskontrolle im Jahr 2008 Wie ist die gegenwärtige Diskussion entstanden?

Für die neue EU-Luftsicherheitsverordnung (EG) 300/2008 (derzeit noch nicht anwendbar) sind Durchführungsbestimmungen erforderlich, die von der Europäischen Kommission (EU-KOM) vorgeschlagen und beschlossen werden.

Eine erste Fassung der geplanten Durchführungsverordnungen war dem Europäischen Parlament (EP) von der Europäischen Kommission kurz vor der Sommerpause 2008 zugeleitet worden. Darin waren u. a. die möglichen Kontrollmethoden aufgelistet, die im Rahmen der detaillierten Durchführungsbestimmungen überhaupt zugelassen werden können; erfasst waren darin auch die so genannten Body-Scanner.

Nachdem sich weiterer Prüfungsbedarf ergeben hatte, hat die Europäische Kommission den Verordnungsentwurf inzwischen wieder zurückgezogen und beabsichtigt, diesen zunächst ohne die Regelung zu den Body-Scannern neu einzubringen. Dem insbesondere von der Deutschen Bundesregierung vorgetragenen Forschungs- und Entwicklungsbedarf soll Rechnung getragen werden.

Es muss ausgeschlossen werden können, dass Persönlichkeitsrechte durch die Art der Bilddarstellung verletzt werden.

Was sind Body-Scanner?

Body-Scanner sind Geräte, die die Sicherheitskontrolle von Personen effizienter gestalten könnten. In einer Sicherheitsschleuse wird ein dreidimensionales Bild erstellt, auf dem die Körperkonturen und am Körper getragene Gegenstände unabhängig von ihrer Materialbeschaffenheit sichtbar gemacht werden.

Body-Scanner sollten aber allenfalls dann zum Einsatz kommen, wenn die gesundheitliche Unbedenklichkeit und die Wahrung der Persönlichkeitsrechte sichergestellt sind. Das Funktionsprinzip nennt sich „Backscatter", was so viel wie Rückstreuung bedeutet. Eingesetzt werden Röntgenstrahlung in geringer Dosis (ältere Geräte) oder Millimeter- bzw. Terahertz-Wellen. Allerdings durchdringen die Strahlen nicht den Körper, sondern werden von ihm und am Körper getragenen Gegenständen wie von einem Spiegel reflektiert. Aus der reflektierten Strahlung werden die Bilder generiert. Die Identität von Personen kann auf den Bildern nicht festgestellt werden.

Der Begriff „Nackt-Scanner" wird verwendet, weil die getragene Kleidung die Millimeter- oder Terahertz-Wellen nicht abschirmen kann und daher die Körperkonturen auf dem generierten 3-D-Bild erscheinen.

Haltung des Bundesinnenministers

Noch im Oktober hatte Bundesinnenminister Wolfgang Schäuble (CDU) diese Scannertechnik noch als „Unfug" bezeichnet, den Deutschland nicht mitmache. Nun heißt es, es werde nach einer Technik geforscht, die verbotene Gegenstände entdecke, ohne dass das entstehende Bild den Passagier „nackt" zeige.

Die nunmehr angekündigten Labortests sollen zeigen, ob Sprengstoffe oder Keramikmesser zu erkennen sind, die ein Passagier am Körper zu verstecken versucht.

Am Flughafen Zürich hatte es eine einmonatige Testphase gegeben, in der ein Scanner erprobt wurde, allerdings nicht mit Passagieren.

In Amsterdam sind 15 Scanner im Einsatz. Die Fluggäste können selbst entscheiden, ob sie sich durchleuchten lassen wollen oder sich der üblichen Kontrolle unterziehen.

Der innenpolitische Sprecher der SPD, Dieter Wiefelspütz, hatte es für „völlig daneben" gehalten, die Scanner auch nur zu testen, weil sie nach Maßgabe des Grundgesetzes nicht erlaubt seien.

Erneute Diskussion ab 1. Weihnachtstag 2009

Bereits im Jahr 2008 wurde über die Einführung von Körperscannern diskutiert.

Das Europa-Parlament hatte die Forderung der Kommission in Brüssel nach EU-weiten Standards für Körperscanner mit großer Mehrheit abgelehnt. Bedenken bestanden im Hinblick auf Gesundheitsrisiken und den Schutz der Intimsphäre. Die Kommission zog ihren Vorschlag zurück.

Noch im Oktober 2008 hatte der ehemalige Bundesinnenminister Wolfgang Schäuble (CDU) diese Scanner-Technik als „Unfug" bezeichnet, den Deutschland nicht mitmache.

Auch der innenpolitische Sprecher der SPD, Dieter Wiefelspütz, hatte es für „völlig daneben" gehalten, die Scanner auch nur zu testen, wie sie nach Maßgabe des Grundgesetzes nicht erlaubt seien.

Nun sind die Körperscanner wieder im Gespräch, nämlich nachdem am ersten Weihnachtstag ein Terrorist den Versuch eines Anschlags auf ein US-Flugzeug über Detroit unternommen hatte. Er hatte, Medienberichten zufolge, den Sprengstoff in seine Unterwäsche eingenäht an Bord geschmuggelt.

Mehrere Abgeordnete des Europa-Parlaments haben ein gemeinsames Vorgehen der EU bei der Einführung von Körperscannern gefordert.

Bundesinnenminister de Maizière (CDU) will die Körperscanner an Flughäfen einsetzen, setzt allerdings voraus, dass Geräte entwickelt würden, die die Persönlichkeitsrechte der Passagiere „vollumfänglich wahren". Ein Gerät, das diese Maßgabe erfülle, soll noch in diesem Jahr vorgestellt werden.

De Maizière erklärt jedoch, dass ein Einsatz dieser Geräte nur infrage komme, wenn sie leistungsfähig und gesundheitlich völlig unbedenklich seien. Bisher gebe es allerdings auch keine Rechtsgrundlage für den Einsatz der Körperscanner.

Peter Schaar, der Datenschutzbeauftragte des Bundes, lehnt den Einsatz von Körperscannern an Flughäfen ab. Ihn

überrascht es, wie schnell Forderungen erhoben werden, ohne dass die grundsätzlichen Fragen geklärt seien.

Zunächst einmal sei Sachaufklärung angebracht. Dazu müsse auch geklärt werden, wie der Sprengstoff durch die Kontrollen geschmuggelt werden konnte und ob die Technologie geeignet sei, solchen Dingen vorzubeugen.

Der Strahlenschutzexperte der Bundesregierung warnte indes vor Gesundheitsrisiken, die von den Körperscannern ausgingen. Die Röntgenstrahlung habe das Gefährdungspotenzial, langfristig Krebs oder Leukämie zu erzeugen.

Das Risiko steige mit jeder Kontrolle für Vielflieger, die häufig gescannt würden.

Wie funktionieren Körperscanner?

Es gibt ein **passives** und ein **aktives** Verfahren:

Der **passive** Scan erfasst nur die natürliche Terahertz-Strahlung des Körpers. Gegenstände unter der Kleidung werden als Schatten erkennbar.

Bei der **aktiven** Methode wird der Körper mit Terahertz-Wellen bestrahlt und aus deren Rückstreuung ein Bild errechnet.

Einige Scanner nutzen zudem Röntgenstrahlen.

Terahertz-Strahlen sind elektromagnetische Wellen, die im Spektrum zwischen Infrarot- und Mikrowellenstrahlung liegen.

1.3 Internetkriminalität

Die Polizei in der vernetzten Welt

„Das Übel kommt nicht von der Technik, sondern von denen, die sie missbrauchen, mutwillig oder auch nur fahrlässig." (Jacques-Yves Cousteau)

Die Begriffe Computerkriminalität, Computerstraftaten, Hightech- und Cyberkriminalität sind gleichbedeutend, da sie die kriminelle Nutzung von Informations- und Kommunikationsnetzen ohne geografische Begrenzung und die Übertragung von nicht/kaum erfassbaren und kurzlebigen Daten bezeichnen.

70 %, d. h. 46,3 Millionen Deutsche nutzen bereits heute das Internet. Das ergab eine Umfrage von TNS Infratest im Auftrag der Initiative D21. Damit nimmt Deutschland einen Mittelplatz im europäischen Vergleich ein. An der Spitze liegt Island mit 90 % Internetnutzern, gefolgt von Schweden (88 %) und den Niederlanden (87 %). Schlusslichter im Vergleich sind Griechenland (38 %), Bulgarien (35 %) und Rumänien (29 %).

In der Europäischen Union (EU) nutzten 2007 bereits 93 % der EU-Unternehmen und 51 % der EU-Bürger das Internet aktiv.

Die Computertechnologie entwickelt sich rasant. Genauso rasant aber wird das Internet für kriminelle Machenschaften missbraucht – von Wirtschaftsspionage über Kinderpornographie bis zu kriminellen Geldgeschäften. Wie viel Datenmaterial in Deutschland illegal über die Server rauscht, ist nicht belegt. London meldete Ende Mai, es sei für Großbritannien mehr als die Hälfte.

Werden wir der Lage noch Herr oder entwickelt sich das Internet zum größten „Tatort" weltweit?

Die Informations- und Kommunikationstechnologie ist eine zentrale Voraussetzung für das Funktionieren unseres Gemeinwesens. Computer und Datennetze bestimmen zunehmend den beruflichen und privaten Alltag. Sie verändern aber auch Verhaltensweisen der Menschen sowie die Arbeits- und Geschäftsprozesse – auch die Arbeit der Strafverfolgungsbehörden wird immer stärker von den neuen Technologien bestimmt, insbesondere, weil das Internet das Erscheinungsbild von Kriminalität nachhaltig verändert. So tauchen vollkommen neue Modi Operandi und Straftaten auf, die an den konventionellen Ländergrenzen nicht Halt machen und grundsätzlich von jedem Ort der Welt aus gegen jeden Computernutzer verübt werden können.

Während die Globalisierung es den internationalen Kriminellen ermöglicht hat, praktisch ohne Grenzen zu agieren, sind Regierungen und Strafverfolgungsbehörden weiterhin auf ihre nationalen Grenzen beschränkt.

Krimineller Netzmissbrauch

Fast 4 Millionen Deutsche wurden bereits Opfer der Cyberkriminellen und erlitten einen finanziellen Schaden.

Der jährlich weltweit von Internetkriminellen verursachte Schaden beläuft sich nach Schätzungen von Experten auf rund 100 Milliarden Dollar. Am meisten sind Banken betroffen. Aber auch politisch motivierte Internetattacken nehmen zu.

Ein Beispiel: Der Konflikt zwischen Russland und Georgien setzte sich im August 2008 auch im Internet fort. Viele Websites von staatlichen georgischen Stellen waren plötzlich nicht mehr erreichbar oder wurden von Hackern verändert. Auch die Homepage des Außenministeriums von Georgien war durch eine Website ersetzt worden, die den georgischen Präsidenten Micheil Saakaschwili als Nazi zeigte.

Darüber hinaus wurden einige georgische Server von tausenden sinnlosen Anfragen überflutet und so in die Knie gezwungen, dass sie und die auf ihnen gehosteten Websites nicht mehr erreichbar waren.

Über die Urheber wurde nur spekuliert. Beobachter gingen davon aus, dass es sich bei diesen Attacken um einen koordinierten, groß angelegten Cyberwar von russischen Hackern handelte.

Es finden nachweislich – und insbesondere im Rahmen der Organisierten Kriminalität – Angriffe auf Informationssysteme statt und es wächst weltweit die Besorgnis über das Potenzial dieser Art von Terroranschlägen. Wir sind sowohl in unserem Lebensstil als auch in unseren europäischen Infrastrukturen sehr verwundbar geworden. Die Täter können nahezu von jedem Winkel der Erde aus über das Netz agieren. Für die Verfolgung sind die Mitgliedstaaten für die in ihrem Hoheitsgebiet oder von einem ihrer Staatsbürger verübten Straftaten zuständig. Falls mehrere Mitgliedstaaten zuständig sind, müssen sie gemeinsam den Mitgliedstaat festlegen, der den Täter der Straftat verfolgt, denn bei grenzüberschreitenden Computerstraftaten ist es wichtig, dass eindeutig festgelegt ist, welches Land für die Strafverfolgung zuständig ist. Vor allem muss vermieden werden, dass sich überhaupt kein Land zuständig fühlt.

Das Strafmaß

Künftig sollen Straftaten, die über das Internet begangen wurden, härter bestraft werden, fordert die Europäische Kommission. Außerdem will sie ein einheitliches Informationssystem in der EU einführen.

Der Missbrauch der neuen Technologien stellt die Polizei und die Rechtsprechung auf der ganzen Welt vor bislang unbekannte Probleme, da sie es mit hoch spezialisierten Kriminellen und mit unglaublich komplizierten Technologien zu tun haben, wobei sich die Kriminellen schnell und professionell neuen technischen Entwicklungen anpassen. Sie reagieren unverzüglich auf technische Sicherheitsvorkehrungen. Die Polizeibehörden können mit den technisch auf höchstem Stand operierenden Organisationen oft nicht mithalten und müssen sich ständig auf neue Internet-Delikte einstellen. Denn das Internet ist – wie vielfach irrtümlich angenommen – eben kein „rechtsfreier Raum". Ziel der freiheitlich demokratischen Grundordnung der Bundesrepublik Deutschland ist es, den Menschen ein selbstbestimmtes, freies Leben zu ermöglichen. Zum Schutz dieser Freiheit haben wir uns daher Gesetze gegeben, die das Leben in seinem Miteinander, Nebeneinander und manchmal Gegeneinander regeln sollen. Auch für das Internet, für die Kommunikation mit Hilfe dieser neuen Techniken, gelten diese Gesetze schon heute. Die Durchsetzbarkeit dieser Gesetze stößt jedoch sehr oft auf technische Hindernisse.

Es besteht also Handlungsbedarf in doppelter Hinsicht:

Zum einen gilt es, durch Verstärkung der Sicherheit von Informationsinfrastrukturen kriminellen Handlungen vorzubeugen, und zum anderen muss dafür Sorge getragen werden, dass die Strafverfolgungsbehörden über geeignete Mittel verfügen, um unter Wahrung der Grundrechte des Einzelnen wirksam gegen derartige Handlungen vorgehen zu können.

Womit wir es im Detail zu tun haben:

In der Fortschreibung des „Programms Innere Sicherheit 2008/2009" differenziert die Innenministerkonferenz die Informations- und Kommunikationskriminalität in

- IuK-Kriminalität im engeren Sinne
- IuK-Kriminalität im weiteren Sinne

IuK-Kriminalität im engeren Sinne:

- widerrechtliches Abgreifen von Daten (Phishing)
- Ausspähen von Daten, Datenveränderung/ -fälschung und Rechnersabotage
- Einsatz von Schadprogrammen („Malware") und Trojaner als Tatmittel zum Angriff auf Rechner und Mobiltelefone
- Nutzung so genannter „Bot-Netze" zur Verschleierung oder Anonymisierung von Täteraktivitäten
- Überlastung von Servern mit massenhaften Anfragen, um zu verhindern, dass deren Inhalte verfügbar sind (DDoS-Angriffe)
- Unberechtigtes Eindringen in Rechnersysteme (Hacking)

  (§ 202 a StGB – Ausspähen von Daten, § 202 b StGB – Abfangen von Daten, § 202 c StGB – Vorbereiten des Ausspähens und Abfangens von Daten, § 263 a StGB – Computerbetrug (Ausnahme: Missbrauch von Zahlungskarten, Missbrauch von Internet-Zugangsdaten), § 269 StGB – Fälschung beweiserheblicher Daten, § 270 StGB – Täuschung im Rechtsverkehr bei Datenverarbeitung, §§ 271, 274 I Nr. 2, 348 StGB – Falschbeurkundung/Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung, § 303 a StGB-Datenveränderung, § 303 b StGB – Computersabotage)

IuK-Kriminalität im weiteren Sinne:

Die Deliktsbreite reicht von der Verbreitung kinderpornografischer Inhalte über das betrügerische Anbieten von Waren und Dienstleistungen, das verbotene Glücksspiel, unlautere Werbung, Urheberrechtsverletzungen bis hin zum illegalen Verkauf von Waffen, Betäubungsmitteln und Medikamenten.

Darüber hinaus nutzen terroristische Netzwerke, extremistische Gruppierungen sowie die Organisierte Kriminalität und Wirtschaftskriminalität die IuK-Technik als Plattform für

- Information und Kommunikation
- Propaganda durch Hetz- und Schmähschriften mit dem Ziel der Radikalisierung und/oder der Bedrohung von Gegnern
- Die Verbreitung von Handlungsanleitungen, auch zum Bau und Einsatz von Sprengvorrichtungen/-fallen
- Rekrutierungen und Anmietungen
- Tatmittelbeschaffung

Cyberwar bedeutet die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus der Informationstechnik. Ziel ist es, die Computersysteme des/der Gegner/s so zu beeinträchtigen, dass sie ihren Zweck nicht mehr erfüllen – z. B. die Kontrolle über Rechnersysteme zu erringen und diese so „umzufunktionieren". So könnte beispielsweise Nichtvorhandenes als Wirklichkeit ausgegeben oder rechnergestützte Führungs- und Waffenleitsysteme gar dazu gebracht werden, die eigenen Kräfte zu treffen.

Umgekehrt gehören zum Cyberwar natürlich die Bereitstellung und Aufrechterhaltung der eigenen Kommunikations- und Kommandostrukturen sowie die Abwehr bzw. Vereitelung gegnerischer Angriffe auf diese.

Methoden des Cyberwar (es kommen laufend neue hinzu!):

- Spionage: Das Eindringen in fremde Computersysteme zum Zwecke der Informationsgewinnung.
- Defacement: Veränderungen am Inhalt einer Website, um u. a. Propaganda zu schalten.
- Denial-of-Service-Attacken: Ein Verbund von Computern attackiert gleichzeitig feindliche Computersysteme, damit diese unter dem Datenstrom zusammenbrechen.
- Social Engineering: Social Egineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus (z. B. die Behauptung, Dienstleis-

tungen wurden nicht bezahlt), um geheime Informationen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man sprich dabei auch vom Social Hacking.

Auch gegen das Computernetz der deutschen Bundesregierung und der Ministerien nimmt die Anzahl von Cyber-Attacken zu. Täglich werden Angriffsversuche auf die Rechner der Bundesregierung festgestellt. Pro Jahr gibt es Hunderte Versuche, Spionageprogramme einzuschleusen – die meisten Angriffe richten sich gegen das Auswärtige Amt.

Allein an den beiden Internet-Schnittstellen des Informationsverbundes Berlin/Bonn registrieren Virenscanner jährlich rund 600 Einschleusversuche für Spionageprogramme per E-Mail, wobei bei weiten nicht alle Angriffe entdeckt werden. Auffallend viele sollen ihren Ursprung in China haben. Es ist sicher noch in Erinnerung, als im August 2007 chinesische Hacker in das Netz des Bundeskanzleramtes eingedrungen waren. Chinesische Angriffe auf deutsche Netze sollen bereits seit Anfang der 90er Jahre nachgewiesen sein.

Elektronische Schädlinge im Netz

Auch die Zahl und Qualität von Computerviren, trojanischen Pferden, Würmern und weiteren Computerschädlingen hat zugenommen. Das Beispiel der letzten Monate ist der Computerwurm „Conficker". Er hat sich seit 2008 weltweit stark ausgebreitet. Anfang 2009 wurde bekannt, dass auch Rechner der Bundeswehr von diesem Schadprogramm angegriffen wurden.

Nach Informationen des Nachrichtenmagazins „Der Spiegel" wappnet sich die Bundeswehr mit einer bisher nicht bekannten Einheit gegen künftige Internet-Konflikte. Diese Einheit soll nicht nur die eigene IT-Infrastruktur vor Angriffen schützen, sondern auch Erkundungen und Manipulationen auf fremden Rechnern bzw. „in gegnerischen Netzen" durchführen. Die Truppe soll aus mehreren Dutzend Informatik-Absolventen der Bundeswehruniversitäten bestehen und in Rheinbach bei Bonn stationiert sein.

Nicht nur Manipulation und Sabotage haben Cyberangriffe zum Ziel. Zunehmend zielen sie auch auf Spionage.

Im März 2009 wurde bekannt, dass kanadische Forscher ein so genanntes „Ghostnet", ein riesiges Spionagenetz, entdeckt haben. Mindestens 1.295 Rechner in 103 Staaten wurden infiltriert.

Rechner mit hohem Informationswert in Außenministerien, Sicherheitsbehörden, Botschaften oder internationale Organisationen waren von den Angriffen besonders betroffen.

Bekämpfung von Kinderpornographie

Am 18. Juni 2009 verabschiedete der Bundestag das „Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen", das auf drei Jahre befristet sein soll. Demnach soll das Bundeskriminalamt (BKA) täglich eine Sperrliste der inkriminierten Web-Seiten erstellen. Alle Zugangsanbieter mit mindestens 10.000 Teilnehmern müssen diese Listen dann „unverzüglich" und zumindest auf Ebene des Domain Name System (DNS) implementieren.

Außereuropäische Kinderporno-Angebote darf das BKA sofort in das Filterverzeichnis aufnehmen, wenn ihm eine Löschbarkeit der Serverinhalte in angemessener Zeit nicht plausibel erscheint. Wenn dann jemand absichtlich oder per Zufall eine Seite aufruft, die in der Sperrliste enthalten ist, erscheint statt der erwarteten Seite ein Stopp-Schild. Die Suche nach der Seite endet dann hoffentlich hier.

Jürgen Vorbeck, Vorsitzender des Bezirks BKA der GdP, kann das nur als kleinen Schritt in die richtige Richtung bewerten, weil die Umgehung dieses Stopp-Schildes leicht möglich ist. Ein echter Fortschritt wäre ein international verbindliches Rechtshilfeabkommen, das die erforderlichen Schließungen der Server, auf denen kinderpornographische Inhalte gespeichert sind, grenzüberschreitend ermöglichen würde.

In Deutschland steigt die Zahl der ermittelten Fälle von Kinderpornographie zwar ständig und erreichte 2007 bereits 11.357 Fälle. Aber nach Einschätzung des BKA können die Straftäter im Internet noch nicht wirksam genug ermittelt und bekämpft werden.

Mit großem Interesse hat der Europarat die Umsetzung des deutschen Gesetzes zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen zur Kenntnis genommen. Es müsse überlegt werden, ob alle Europarat-Staaten technische Web-Blockaden implementieren sollten.

Internationale Zusammenarbeit auf Staatsebene

Um die Internetkriminalität einzudämmen, ist eine intensive internationale Zusammenarbeit auch auf staatlicher Ebene notwendig. Denn solange Cyberkriminalität nicht grenzüberschreitend strafrechtlich erfasst wird, ist eine internationale Verfolgung unmöglich!

Eindringlichste Beispiele dafür sind solche Seiten im Internet, auf denen gewaltverherrlichende, rechtsextremistische oder pornographische Inhalte über das Internet verbreitet werden. Die Inhalte werden häufig über Rechner in das Internet eingestellt, die sich in den USA befinden. Bei der komplizierten Rückverfolgung der Spuren, die auf die Anbieter solcher Internetseiten hinweisen, stoßen die Strafverfolgungsbehörden in Deutschland regelmäßig an ihre rechtlichen Grenzen. In den USA sind viele der bei uns strafrechtlich relevanten Tatbestände durch die dort sehr weit ausgelegte Meinungsfreiheit geschützt. Ein Rechtshilfeersuchen scheitert in solchen Fällen meist daran, dass die USA nur Rechtshilfe bei solchen strafrechtlichen Ermittlungen gewährt, in denen die Tatbestände nicht nur in Deutschland, sondern auch in den USA unter Strafe gestellt sind. Ein Zustand, der für jeden, der eine solche Internetseite einmal gesehen hat, unerträglich und nicht hinnehmbar ist. Juristisch bestehen jedoch keine Möglichkeiten, dagegen vorzugehen.

Auch rein praktisch dürfte die weitere Verbreitung solcher Seiten in Deutschland und damit der freie Zugang über das Internet kaum zu verhindern sein. Im Internet herrscht die Philosophie vor, dass jegliches Eingreifen als Zensurmaßnahme eingestuft, als Störung empfunden und darauf mit einer Umleitung reagiert wird. Selbst wenn also einzelne Provider in Deutschland sich weigern würden, die entsprechenden Seiten weiterzuleiten, würden sich sicherlich andere, weniger namhafte Anbieter finden, die stattdessen die Seiten weiterleiten. Auch die User würden sicherlich in solchen Fällen verstärkt versuchen, genau auf diese Seite zurückzugreifen,

nicht der Inhalte wegen, die sie vielleicht im Einzelfall auch ablehnen mögen, aber infolge der Grundphilosophie.

Wer im Internet Straftaten verüben will, der braucht nur „für sein Bedürfnis" einen Weg durch die Datenmenge zu finden. Die Sicherheitsbehörden hingegen müssen den Einzelnen auf die Spur kommen, aber auch relevante Systeme vor Eindringlingen und die Bürgerinnen und Bürger vor kriminellen Web-Attacken schützen. Ein Feld, das in den kommenden Jahren dringend hohe Fachkompetenz, staatliche Zusammenarbeit und Rechtssicherheit erfordert.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Mit dem Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik vom 17. Dezember 1990 wurde bereits 1991 das Bundesamt für Sicherheit in der Informationstechnik (BSI), eine Bundesoberbehörde, als zentraler Dienstleister für die IT-Sicherheit der Bundesverwaltung geschaffen. Das BSI untersteht dem Bundesminister des Innern.

IT-Sicherheit ist längst ein integraler Bestandteil der Inneren Sicherheit geworden, aber auch im privaten Alltag immer intensiver präsent. Vom Bankautomaten über die Energie- und Wasserversorgung bis hin zu Flug- und Bahnhöfen ist die IT-Infrastruktur von zentraler Bedeutung für das Gemeinwesen. Angriffe auf diese Infrastruktur können immense Schäden anrichten, bis zu Katastrophen führen.

Weil die Probleme in der Informationstechnik so vielschichtig sind, ist auch das Aufgabenspektrum des BSI sehr komplex: Es untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik, spürt Sicherheitslücken auf und entwickelt Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und sucht Lösungen dafür.

Auch bei technisch sicheren Informations- und Telekommunikationssystemen können Risiken und Schäden durch unzureichende Administration und Anwendung entstehen. Um diese Risiken zu minimieren beziehungsweise zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen: Es berät Hersteller, Vertreiber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

Novellierung des BSI-Gesetzes

Mit dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes, das der Deutsche Bundestag am 18. Juni 2009 verabschiedet hat, werden dem BSI als zentrale Meldestelle für IT-Sicherheit Befugnisse eingeräumt, in Sachen IT-Sicherheit Informationen zu Sicherheitslücken, Schadprogrammen oder Angriffen zu sammeln und auszuwerten. So können Angriffe und Angriffsmuster besser erkannt und Gegenmaßnahmen eingeleitet werden.

Das BSI darf künftig zur Bekämpfung von Schadprogrammen alle Protokolldaten, einschließlich personenbezogener Nutzerinformationen wie IP-Adressen, die bei der Online-Kommunikation zwischen Bürgern und Verwaltungseinrichtungen des Bundes anfallen, unbegrenzt speichern und auswerten. Im Kern geht es darum, dass das BSI mit seinen Möglichkeiten eine Art Schadprogrammscanner über den Datenverkehr der Bundesbehörden legt. So sollen Schadprogramme erkannt und abgewehrt werden können.

Eine zu protokollierende Entpseudonymisierung oder Weitergabe von Daten an Sicherheitsbehörden darf nur bei Straftaten erfolgen, die mittels Schadprogrammen begangen wurden, konkret: das Ausspähen und Abfangen oder das Verändern von Daten oder Computersabotage. Auch die Weitergabe (nur mit richterlicher Zustimmung) bei der Verfolgung erheblicher Straftaten, insbesondere im Sinne des § 100 a Abs. 2 StPO, also z. B. Mord oder Totschlag, ist möglich.

Darüber hinaus kann das BSI technische Vorgaben und verbindliche Mindeststandards für die Sicherheit der Informationstechnik in der Bundesverwaltung machen – das betrifft auch Richtlinien für die Beschaffung von IT-Produkten – und es kann private IT-Dienstleister prüfen und zertifizieren sowie deren Eignung und Zuverlässigkeit bestätigen. Das ist für Wirtschaft und Verwaltung gleichermaßen von Bedeutung, da Unternehmen und Behörden zunehmend Komplettlösungen kaufen, die bis zur vollständigen Auslagerung der IT reichen. Die Prüfung von Kompetenz und Vertrauenswürdigkeit eines Dienstleisters soll hier einen erheblichen Qualitätsschub bewirken.

Zu den Aufgaben des BSI gehören gemäß § 3 BSIG u. a.:

Unterstützung

1. der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben,
2. der Verfassungsschutzbehörden bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder anfallen.
3. des Bundesnachrichtendienstes bei der Wahrnehmung seiner gesetzlichen Aufgaben.

Die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen.

CERT-Bund – Das Computer-Notfallteam des Bundes

Computer-Notfallteams, CERTs (Computer Emergency Response Teams) genannt, sind das Mittel, um schnell und zuverlässig bei erkannten Gefährdungen und Risiken im Bereich der Informations- und Kommunikationstechnik (IuK) agieren und auf IT-Sicherheitsvorfälle reagieren zu können. Die wiederholten Angriffe auf IT-Netze und Endsysteme, beispielhaft genannt werden DDoS-Angriffe und Computer-Viren, haben die Notwendigkeit der Einrichtung einer zentralen Anlaufstelle zur Lösung von Problemen der Rechner- und Netzwerksicherheit für den Bereich des Bundes verdeutlicht.

So wurde am 01. September 2001 im Rahmen der Neuorganisation des BSI das Referat CERT-Bund („Computer Emergency Response Team für Bundesbehörden") neu aufgestellt. Dadurch wurde das ehemalige BSI-CERT in eine eigene Organisationseinheit überführt und die wahrzunehmenden Aufgaben überarbeitet und neu definiert.

CERT-Bund übernimmt aus dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen" die Aufgabe, das

Krisenreaktionszentrum IT des Bundes aufzubauen und innerhalb dessen das nationale Frühwarnsystem zu betreiben.

Die Dienstleistungen von CERT-Bund stehen in erster Linie den Bundesbehörden zur Verfügung, Anfragen von Privatpersonen oder privaten Institutionen werden im Rahmen verfügbarer Ressourcen bearbeitet.

Die European Government CERTs (EGC) Group

Die EGC-Gruppe ist ein informeller Zusammenschluss europäischer Behörden-CERTs. Ziel ist die Entwicklung einer effektiven Kooperation in Bezug auf IT-Sicherheitsvorfälle (engl. Incident Response). Ausgangspunkte des gemeinsamen Handelns sind dabei gleichartige Interessen der Mitglieder aufgrund ähnlicher Zielgruppenstrukturen und Problemlagen.

Gegenwärtig sind Mitglied der EGC-Gruppe: Finnland (CERT-FI), Frankreich (CERTA), Deutschland (CERT-Bund), Ungarn (CERT-Hungary), Niederlande (GOVCERT.NL), Norwegen (NorCERT), Schweden (SITIC), United Kingdom (CSIR-TUK), United Kingdom (GovCertUK).

BSI für Bürger

Für alle, die sich über die Gefahren im Internet informieren möchten, hält das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Infoportal www.bsi-fuer-buerger.de bereit. Hier werden auch für Technik-Laien verständlich die Risiken der digitalen Welt erklärt und Tipps zum Schutz gegen die wachsenden Internet-Gefahren gegeben.

Bürger-CERT

Der Bürger-CERT-Newsletter informiert und warnt Bürger und kleine Unternehmen schnell und kompetent vor Viren, Würmern und Sicherheitslücken in Computeranwendungen – kostenfrei und absolut neutral. Die Experten des BSI analysieren für die Bürger rund um die Uhr die Sicherheitslage im Internet und verschicken bei Handlungsbedarf Warnmeldungen und Sicherheitshinweise per E-Mail. Das Bürger-CERT ist ein Projekt des BSI.

1 Quelle: www.bsi.de

2 Quelle: www.bsi.de

Bedrohungen durch das World Wide Web – Schutz kritischer Infrastruktur

So lautete der Titel eines Kongresses, der am 30. November und 01. Dezember 2009 in der Bundesakademie für Sicherheitspolitik (BAKS) in Zusammenarbeit mit T-Systems in Berlin stattgefunden hat.

Zum dritten Mal hatte die Bundesakademie für Sicherheitspolitik gemeinsam mit T-Systems zahlreiche Experten eingeladen, um Themen der globalen Kommunikation und Informationstechnologie zu diskutieren.

Den Vortrag zur Einleitung in das Kongressthema hielt MinDir Martin Schalbruch, IT-Direktor im Bundesinnenministerium (BMI). Er ging auf die vielfältigen Gefahren, die das Internet bietet ein, und hob insbesondere die zunehmende Zahl von Bot-Netzen, die für vielfältigste kriminelle Aktionen genutzt werden, hervor.

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Michael Hunge, warnte vor dem Irrglauben, dass es im Internet auch nur irgendeine Vertraulichkeit gebe. Mit eindeutigen Identitäten sei es im Internet weit her. Vielfach würden falsche Identitäten genutzt, um illegale Geschäfte über das Internet abzuwickeln.

Identitätsdiebstahl durch Schadsoftware findet in einer Vielzahl von Branchen statt.

Seit 2005 werden auch in Deutschland auf breiter Basis gegen öffentliche Einrichtungen und Wirtschaftsunternehmen gerichtete Angriffe über das Internet mit unterschiedlichster Motivation beobachtet. Neben der Absicht, Aufmerksamkeit zu erregen oder den Betroffenen Schaden zuzufügen, stehen zunehmend die Erzielung wirtschaftlicher Vorteile oder eine politische Motivation im Mittelpunkt. Benutzt werden die Begriffe Cyber-Crime, Cyber-Terrorismus und Cyber-Warfare.

Die gängigste Angriffsmethode und größte Bedrohung besteht in der Versendung von E-Mails, die mit einem Schadprogramm-„verseuchten“ Anhang versehen sind. Sobald ein solcher Anhang geöffnet wurde, treibt das Schadprogramm fortan auf dem infizierten Rechner sein Unwesen, ohne dass der Benutzer es unbedingt bemerkt.

Eine Infektion durch Schadprogramme erfolgt aber nicht nur über E-Mail, sondern auch über infizierte Webseiten oder über Datenträger, wie USB-Sticks oder CDROM bzw. DVD. Infizierte Rechner können dann auch über verteilte Kontrollstrukturen, wie Botnetze ferngesteuert werden.

Die kritische Situation permanenter Cyber-Attacks eskaliert weiter. Gängigste Angriffsmethoden sind: Hacking, Viren, Würmer, Trojaner, Phishing, DDOS-Attacken und Social Engineering. Intelligenz und Kriminalität haben sich hier gepaart und zum gegenwärtigen Zeitpunkt werden die Strafverfolger offensichtlich nicht Herr der Lage. Die Zahl erfolgreicher Angriffe steigt nämlich rapide. Monatlich werden Millionen von digitalen Identitäten gestohlen sowie Bot-Netze mit mehreren Millionen gekaperten Rechnern gebildet. Auch die Spionagenetze (Ghost-Nets) nehmen zu.

Die Softwareindustrie produziert „Trojanerbaukästen“, die über diverse Kanäle vertrieben werden und auch Ungeübten die Möglichkeit eröffnen, Trojaner gezielt für eigene Zwecke einzusetzen. Die meisten Trojaner laufen an den Virenscannern vorbei, d. h., sie werden von ihnen nicht erkannt. Der Identitätsdiebstahl und die Identitätsfälschung werden für kriminelle Machenschaften genutzt.

Bot-Netze können zwischenzeitlich über das Internet für vielfältigste Zwecke angemietet werden.

Spionagenetze dienen nicht nur der Wirtschaftsspionage. Gezielte Spionageangriffe finden täglich statt. Betroffen sind auch Computer von Banken, Botschaften, Außenministerien und anderen Regierungsstellen.

Nachhaltige Erfolge bei der Bekämpfung der Cyber-Attacks sind nur durch Zusammenarbeit aller Beteiligten zu erreichen.

Dazu zählen die Kreditinstitute, Strafverfolgungsbehörden, Internetzugangsanbieter und die Antivirenindustrie.

Auch der internationale Terrorismus profitiert von der Komplexität und Globalität des Netzes. Ideologietransfer und Radikalisierungsprozesse werden rein virtuell kommunizierbar, waffentechnologische Anleitungen weltweit zugänglich.

„Die virtuelle Welt setzt andere Rahmenbedingungen für kriminelles Verhalten als die reale Welt. Während in der realen Welt bei der Verfolgung von Straftaten häufig noch allgemeine Personen- und Sachbeweise geeignete Ermittlungsansätze bieten, stellen die im Internet vom Täter hinterlassenen elektronischen Spuren überwiegend den eigentlichen Ermittlungsansatz dar. Verschlüsselungsmethoden und die Flüchtigkeit solcher ermittlungsrelevanten Daten stellen die Strafverfolgungsbehörden vor besondere Herausforderungen. Das erfordert jedoch neue Bekämpfungsstrategien und -maßnahmen“ (F-M. Silberbach, BKA-SO 43).

2. Mitbestimmung

2.1 Foren für die Vorsitzenden der Haupt- und Gesamtpersonalräte in der Polizei

Forum für die Vorsitzenden der Haupt- und Gesamtpersonalräte 2007

In der zweiten Jahreshälfte 2007 wurde im Zusammenhang mit dem Schöneberger Forum in Berlin ein Forum für die Vorsitzenden der Haupt- und Gesamtpersonalräte in der Polizei durchgeführt.

Forum für die Vorsitzenden der Haupt- und Gesamtpersonalräte 2008

Am 11. / 12. Dezember 2008 fand ein weiteres Forum für die Vorsitzenden der Haupt- und Gesamtpersonalräte in der Polizei in Kassel statt. Das Programm beinhaltete u. a. folgende Themen:

Personalrat und GdP / GdP und Personalrat
- aktuelle Gewerkschaftspolitik und vertrauensvolle Zusammenarbeit

Personalgestellung durch die deutsche Polizei bei internationalen Missionen / Auslandseinsätze der deutschen Polizei
- Rolle der Personalvertretungen / Personalvertretungsrechtliche Beteiligung

Arbeitszeitrecht in der Polizei
- Forschungsprojekt Lebensarbeitszeit
- Gutachten zu der Anwendungsfrage RiLi 2003/88/EG

Gestaltung der Arbeitsplätze
- in Dienstfahrzeugen
- in Dienststellen

Die Teilnehmer hatten auch Gelegenheit, mit dem Bundesvorsitzenden über aktuelle Gewerkschaftspolitik zu diskutieren. Themen waren u. a. die Chancen und Risiken der Finanzmarktkrise, die Bundestagswahl, der Skandal bei der T-Com, die zunehmende Gewalt gegen Polizisten, zurückliegende Personalratswahlen sowie die Ergebnisse und die Mitgliederentwicklung.

2.2 Freistellung und Kostenübernahme für Schulungs- und Bildungsveranstaltungen nach § 46 Abs. 6 BPersVG

Das Bundesinnenministerium hatte u. a. alle obersten Bundesbehörden, aber auch die Spitzenorganisationen um Stellungnahme zu dem Entwurf eines neuen Rundschreibens gebeten.

Das Bundesinnenministerium begründet die Neufassung des Rundschreibens wie folgt:

Das bisherige Rundschreiben „Kosten der Teilnahme an Schulungs- und Bildungsveranstaltungen im Sinne des § 46 Abs. 6 Bundespersonalvertretungsgesetz (BPersVG)“ bedarf aus folgenden Gründen einer Überarbeitung:

a) Der Pauschbetrag – der seit 1996 unverändert ist – soll von derzeit 102,26 Euro auf

b) 125 Euro angehoben werden.

c) Bei der Auswahl und Durchführung von Schulungs- und Bildungsveranstaltungen sollen auch innovative Bildungskonzepte, wie z. B. Online-Seminare / E-Learning-Angebote, Fernlehrgänge sowie Indoor- / Inhouse-Schulungen berücksichtigt werden und ggf. zu einer Entlastung des Haushalts beitragen.

d) Die Rechtsprechung seit Einführung des Rundschreibens im Jahre 1996 insbesondere durch das Bundesverwaltungsgericht und das Bundesarbeitsgericht sowie durch die Oberverwaltungsgerichte bzw. die Verwaltungsgerichtshöfe ist zu berücksichtigen.

e) Schließlich ist die Änderung des Bundesreisekostengesetzes (BRKG) in das Rundschreiben einzuarbeiten.

Aufgrund der Zahl der Änderungen habe ich eine grundlegende Neufassung vorgesehen.

Die GdP begrüßt das Vorhaben des Bundesinnenministeriums, den Pauschbetrag für Schulungs- und Bildungsveranstaltungen im Sinne des § 46 Abs. 6 BPersVG anheben zu wollen.

Eine Anhebung auf 125 Euro ist allerdings nicht ausreichend, um kostendeckende Schulungsveranstaltungen durchführen zu können. Es müsste seitens der Gewerkschaften weiterhin „spitz“ abgerechnet werden, was letztlich nicht zu der angestrebten Verwaltungsvereinfachung führen wird.

Die GdP lehnt Indoor- und Inhouse-Schulungen grundsätzlich ab.

E-Learning kommt für die GdP nur nach einer Grundschulung und auch nur dann in Betracht, wenn die technischen Grundvoraussetzungen geschaffen wurden, d. h. ein diskreter Zugang zu einem E-Learning-Programm über ein ständig verfügbares EDV-System mit der notwendigerweise angeschlossenen Peripherie.

2.3 Projekt „Mitbestimmung & Teilhabe“ der Initiative Trendwende des DGB

Das Projekt „Mitbestimmung & Teilhabe“ der „Initiative Trendwende“ des DGB gliedert sich in zwei Teilprojekte:

1. MAA = Mitbestimmung am Arbeitsplatz und
2. MAB = Mitbestimmung und materielle Arbeitnehmerbeteiligung

Ziel des Teilprojektes MAB ist es, das Zukunftsthema „Materielle Arbeitnehmerbeteiligung“ durch den DGB und seine Mitgliedsgewerkschaften kompetent zu besetzen.

Im Januar 2007 fand die erste Sitzung der Teilprojektgruppe MAB statt. Die Teilnehmer von DGB, IGM, IGBCE, NGG, ver.di, Transnet hatten sich ein Arbeitsprogramm gegeben. Die GdP war anfänglich in dieser Teilprojektgruppe nicht vertreten.

Bis Herbst 2007 sollte ein gewerkschaftliches Positionspapier zu MAB entstehen.

In der Juni-Sitzung 2007 wurde der Steuerungsgruppe das Projekt „Mitbestimmung & Teilhabe“ vorgestellt und der Auftrag für das Teilprojekt MAB geklärt. Als ein wichtiges Ergebnis wurde in der Steuerungsgruppe festgehalten, dass MAB ein Zukunftsthema ist und von den Gewerkschaften im Projekt diskutiert werden soll.

Daraus ergab sich die Konsequenz, dass die Projektgruppe MAB um die bis dahin nicht beteiligten Gewerkschaften GdP, GEW, IG BAU erweitert wurde.

Die GdP nahm das Positionspapier aus der Projektgruppe MAB des Projekts „Mitbestimmung & Teilhabe“ des DGB zustimmend zur Kenntnis.

2.4 Personalrätebefragung durch das WSI im Jahr 2007

Ergebnisübersicht:

Das WSI hat im Jahr 2007 in telefonischen Interviews, die durchschnittlich 50 Minuten dauerten, 1.742 Personalräte in Dienststellen mit über 20 Beschäftigten befragt.

Von den Befragten haben sieben das Gespräch abgebrochen. 92 % der Befragten würden sich noch einmal an einer solchen Umfrage beteiligen.

Anzumerken ist auch, dass erstmals die Befragung von Betriebs- und Personalräten getrennt durchgeführt wurde.

Die Ergebnisse sehen wie folgt aus:

Viele Personalratsmitglieder haben Angst, aufgrund ihrer Freistellung zu den fachlichen Themen ihres Berufslebens den Kontakt zu verlieren. Sie befürchten deshalb beim Wiedereinstieg nach der Amtszeit Schwierigkeiten oder einen Karriereknick.

Das wird auch daran erkennbar, dass die rechtlich zulässige Freistellungsquote von rund 30 % der befragten Personalräte nicht ausgeschöpft wird. 45 % schöpfen die Quote voll aus.

Warum werden Freistellungsmöglichkeiten nicht voll ausgeschöpft?

9 % der Freistellungsanträge wurden nicht bewilligt, 78 % der Personalräte hatten nicht mehr beantragt, 51 % der Personalratsmitglieder wollen ihre dienstliche Tätigkeit für den Personalrat nicht einschränken, 46 % sind der Auffassung, dass die in der Dienststelle anfallenden Personalratstätigkeiten keine weiteren Freistellungen rechtfertigen.

Um diesen Sorgen abzuhelfen, sind ergänzende gesetzliche Regelungen zu schaffen, z. B. ein Anspruch ausscheidender Personalratsmitglieder auf Schulungen zur Wiedereingliederung in das Berufsleben. Hierfür soll sich der DGB in einer Initiative starkmachen.

Die Frauenquote bei den Personalratsvorsitzenden beträgt 41 %.

Festgestellt werden konnte auch die durchschnittliche Zahl der Amtsperioden eines Personalrats:

Vorsitzende werden im Schnitt nach 1,6 Amtsperioden in dieses Amt gewählt und sind dann maximal zwei Amtsperioden Vorsitzender. Das Durchschnittsalter der Personalratsvorsitzenden beträgt 48 Jahre.

Die befragten Personalräte sehen für sich folgenden Qualifikationsbedarf:

1. Tarifvertragsrecht
2. Individualarbeitsrecht
3. Konfliktmanagement / Mediation
4. Gesundheits- und Arbeitsschutz
5. Personalvertretungsrecht
6. Verwaltungsrecht
7. Präsentation – Auftreten
8. Allgemeine Geschäftsführung des Personalrats (in dieser Reihenfolge)

Nach Auffassung der Personalräte wird der Schulungsbedarf durch die Gewerkschaften nicht ausreichend abgedeckt!

32 % der Personalratsmitglieder sagen, das ungenügende Mittel für Qualifizierungsmaßnahmen zur Verfügung stehen.

Räumlich und materiell sahen sich die Personalräte gut ausgestattet.

Organisationsgrad der Beschäftigten:

DBB	41 %
ver.di	21 %
GEW	30 %
GdP	60 %

Organisationsgrad im PR-Gremium (DGB/DBB/keine)

DBB	21/48/31 %
ver.di	53/7/40 %
GEW	41/15/44 %
GdP	73/21/6 %
DGB gesamt	52/8/39 %

In der AG Personalvertretungsrecht des DGB wurde auch über die Datenlage in den Personalvertretungen diskutiert. Es wurde nämlich deutlich, dass es keine genauen Angaben über die Zahl und Zusammensetzung von Personalvertretungen gibt. Auch die Rückmeldungen der Personalräte an die Gewerkschaften nach einer Wahl sind lückenhaft. Daher wurde erörtert, ob sich der DGB für ein gesetzliches Register starkmachen soll, demgegenüber das Bestehen einer Personalvertretung und deren Zusammensetzung zu melden ist.

2.5 „Deutscher Personalräte-Preis“ 2010

Der Bund-Verlag beabsichtigt, über die Zeitschrift „Der Personalrat“ 2010 erstmals den „Deutschen Personalräte-Preis“ auszuloben. Ende 2010 soll dieser Preis im Rahmen des „Schöneberger Forums“ verliehen werden.

Die GdP wurde um Unterstützung für diesen Preis gebeten. Als Mitglied für die Jury möchte der Bund-Verlag das für Mitbestimmung zuständige Mitglied der Einzelgewerkschaften gewinnen.

Der „Deutsche Personalräte-Preis“ steht unter dem Motto „Innovative Personalratsarbeit auch in schwierigen Zeiten“ und wird in Zeitschriften, Internetseiten und Newslettern des Bund-Verlages sowie weiteren Verteilern prominent beworben.

Mit der Verleihung des Personalräte-Preises will die Zeitschrift „Der Personalrat“ die wertvolle, innovative Arbeit würdigen, die Personalräte gerade auch in schwierigeren Zeiten im öffentlichen Dienst leisten. Neben der Wertschätzung für einzelne ausgezeichnete konkrete Projekte wird damit auch der Personalratsarbeit im Allgemeinen mehr Anerkennung verschafft.

Die Auszeichnung Einzelner soll Personalräte motivieren, sich weiter aktiv, kreativ und gestaltend für die Beschäftigten und deren Belange zu engagieren.

Es wird bewusst kein Geldpreis verliehen, sondern ein „Ehrenpreis“ samt Urkunde, der die Wertschätzung und die Anerkennung für die Arbeit der Personalräte zum Ausdruck bringt.

Die GdP unterstützt das Vorhaben des Bund-Verlages, 2010 einen „Deutschen Personalräte-Preis“ zu verleihen.

Als Jury-Mitglied der GdP wurde das für Mitbestimmung zuständige GBV-Mitglied, Jörg Radek, dem Bund-Verlag benannt.

2.6 Betriebs- und Personalrätekonferenz der SPD-Bundestagsfraktion am 22. April 2009

In fast regelmäßigen Abständen lädt die SPD-Bundestagsfraktion Betriebs- und Personalräte zum Dialog zu aktuellen Themen ein. So auch im April 2009 zum Thema

„Schutzschirm für die Beschäftigung“.

Eröffnet und moderiert wurde die Konferenz durch Andrea Nahles, MdB, Arbeits- und sozialpolitische Sprecherin der SPD-Bundestagsfraktion. Die aktuelle Krise in den Finanzmärkten mit ihren massiven Folgen für die Realwirtschaft sei für alle eine große Herausforderung. Der bevorstehende Abschwung bedrohe viele Arbeitsplätze.

Sie forderte, eine soziale Fortschrittsklausel für Europa zu verankern und für Deutschland einen neuen sozial regulierten Kapitalismus, mehr Initiativrechte bei Umstrukturierungen. Vor kurzem habe man noch heftig für den Erhalt des VW-Gesetzes gerungen, und nun sei die Situation eingetreten, dass Banken verstaatlicht würden.

Nahles kündigte eine Konferenz zum Arbeitnehmerdatenschutz an, zu der die SPD in Kürze einladen werde. Der Bundesarbeitsminister werde noch vor der Wahl einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorlegen.

Ferner werde die SPD die Initiative ergreifen, dass die Altersteilzeitregelung verlängert und eine Mindestrente gesetzlich geregelt werde. Die Krise wolle man durch eine gute Mitbestimmungskultur bewältigen.

Es gehe jetzt darum, klarzumachen, dass langfristiges Denken, Sicherung von Arbeitsplätzen, Anerkennung der Arbeit durch Mitsprache im Betrieb auf der Tagesordnung stehen.

Die Konjunkturpakete seien erforderlich, um Arbeitsplätze zu erhalten. Mitbestimmung, die viele Marktradikale in den letzten Jahren noch abschaffen wollten, sei wichtiger denn je.

Mit dem zweiten Konjunkturpaket würden weitere Maßnahmen für eine langfristige starke deutsche Wirtschaft auf den Weg gebracht. Dazu gehören eine Infrastruktur, gute Bildung und lebenslange Qualifizierung. Wichtig sei, dass die Beschäftigten nicht entlassen, sondern qualifiziert und entlassene Arbeitnehmer so schnell wie möglich wieder vermittelt werden.

2.7 Arbeitnehmerdatenschutz

Entschließung des Bundesrates vom 12. September 2008 zur eigenständigen gesetzlichen Ausgestaltung des Arbeitnehmerdatenschutzes

Der Bundesrat hat die Bundesregierung angesichts der Vorfälle von Arbeitnehmerüberwachung in Unternehmen und der für Arbeitgeber wie Arbeitnehmer unübersichtlichen Gesetzeslage gebeten, einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorzulegen. Dieser soll die Grenzen zulässiger Datenerhebung, -verarbeitung und -verwendung klar definieren und für alle Beteiligten Rechtssicherheit schaffen.

Begründung:

Fortlaufend werden Informationen zum Beschäftigtenverhalten aus Internet-, E-Mail- oder Telefondaten, PC-Arbeiten, Zeiterfassungen, Navigationssystemen, Chipkarten oder Kamerabeobachtungen registriert. Hinzu kommen Dokumentationen von ärztlichen Untersuchungen, biometrischen- oder motosensorischen Aufnahmen. Diese Informationen zu sammeln und auszuwerten bereitet technisch keine nennenswerten Schwierigkeiten. Die benötigten Hilfsmittel sind ebenso marktgängig wie erschwinglich.

Wenig Unterschied macht es auch, ob Informationen gezielt oder eher zufällig entgegengenommen werden.

In der jüngsten Vergangenheit sind wiederholt Fälle von Arbeitnehmerüberwachung offenkundig geworden, die eklatant die Würde von Arbeitnehmerinnen und Arbeitnehmern missachtet und gegen die informationelle Selbstbestimmung verstoßen haben. Neben der Willkür des Arbeitgebers, die Beschäftigten in unzulässigerweise zu überwachen und über ihre Arbeitsleistung hinaus zu kontrollieren, spielt die Unwissenheit über bestehende gesetzliche Regelungen und über die Rechtsprechung eine große Rolle. Arbeitnehmer und Arbeitgeber müssen ihre Rechte und die Grenzen des Umfangs und der Verwendung von Arbeitnehmerdaten kennen. Dieses ist nur mit einem übersichtlichen, zusammenfassenden Gesetz zu gewährleisten. Auch die Beauftragten des Bundes und der Länder für Datenschutz fordern den Entwurf eines Arbeitnehmerdatenschutzgesetzes.

Die bestehenden Regeln zum Datenschutz in Arbeitsverhältnissen sind unzulänglich. Auf Bundes- und EU-Ebene sind hierzu nur vereinzelt begleitende Regelungen ergangen.

Die arbeitsrechtliche Praxis orientiert sich überwiegend an Normen, die – bis auf wenige Ausnahmen – nicht speziell auf die Interessenlagen im Arbeitsverhältnis zugeschnitten sind. Innerbetriebliche Regelungen zwischen Arbeitgebern und Interessenvertretungen der Beschäftigten schaffen keine vollständige Abhilfe. Teils gibt es in Betrieben keine Beschäftigtenvertretung. Teils verstehen sich die abgeschlossenen Vereinbarungen eher als anlassbezogene Klärung von Detailfragen.

Eine praktikable, verständliche Gesetzesregelung zum Arbeitnehmerdatenschutz muss die Prinzipien der Transparenz, der Erforderlichkeit und Verhältnismäßigkeit, der legitimen Zweckbindung wie auch der Datensparsamkeit und

-sicherheit berücksichtigen.

Kernelement eines effektiven Arbeitnehmerdatenschutzes muss die sachgerechte Begrenzung der Verarbeitung von Arbeitnehmerdaten sein mit strengen Zweckbindungs- und Verwertbarkeitsregelungen. Ebenso grundlegend ist die Achtung der grundgesetzlich geschützten Persönlichkeitsrechte. Weiterhin ist an eine Stärkung der institutionellen Rechte von betrieblicher Interessenvertretung und Betriebsbeauftragten für Datenschutz zu denken, sind die modernen Kommunikations- und Auswertungstechniken in einen Gesetzesvorschlag aufzunehmen wie auch zureichende Informations-, Kontroll- und Sanktionsregelungen einzuführen.

3. Verwaltungsmodernisierung

3.1 Sitzungen des BFA Polizeiverwaltung

Im Berichtszeitraum fanden folgende Sitzungen des BFA Polizeiverwaltung statt:

02.–03.08.2007	Berlin
23.–24.04.2008	Potsdam
08.–09.10.2008	Kassel
23.–25.06.2009	Workshop BFA in Schönberg/Kalifornien
06.–07.10.2009	Workshop AK des BFA in Potsdam

3.2 Positionspapier „Facility Management und Privatisierung in der Polizei“

Der Bundesvorstand hat in seiner Klausurtagung vom 27. Februar bis 01. März 2007 u. a. beschlossen, die Ad-hoc-Kommission „Facility Management und Privatisierung in der Polizei“ einzurichten.

Die Kommission hat am 26./27. Juli 2007 getagt und beiliegende Positionsbeschreibung zu „Facility Management und Privatisierung in der Polizei“ erarbeitet.

Diese Positionsbeschreibung war auch Gegenstand der Erörterung in der konstituierenden Sitzung des Bundesfachausschuss Polizeiverwaltung am 02./03. August 2007.

Beschluss:

Die durch die Ad-hoc-Kommission erarbeitete Positionsbeschreibung „Facility Management und Privatisierung in der Polizei“ wurde dem Bundesvorstand zu seiner Sitzung am 19./20. September 2007 vorgelegt und zustimmend zur Kenntnis genommen.

3.3 Positionen der GdP zur Polizeiverwaltung

In zwei Workshops hat der BFA Polizeiverwaltung das Positionspapier zur Polizeiverwaltung entwickelt, das nach entsprechender Abstimmung und Berücksichtigung von Ergänzungs- und Änderungswünschen nunmehr in der abschließenden Fassung vorliegt und die Positionen zur Polizeiverwaltung von Juli 2005 ergänzen sollen.

Die Positionen der Polizeiverwaltung – Stand: Dezember 2009 – wurden vom Bundesvorstand in seiner Sitzung im Februar 2010 zustimmend zur Kenntnis genommen.

3.4 Positionspapier „Versorgung im Einsatz“

Einrichtung einer Arbeitsgruppe „Versorgung im Einsatz“

Der Ergebnisbericht über die Nachbereitung des G-8-Gipfels in Heiligendamm offenbart neben alarmierenden Hinweisen über die Unterbringung und Diensteinteilungen von Einsatzkräften auch gravierende Mängel in der Versorgung.

Es gibt zwar einen Anforderungskatalog über einzuhaltende Mindeststandards bei Großeinsätzen, der auch unter Mitwirkung der GdP erstellt wurde. Jedoch muss festgestellt werden, dass immer wieder Umsetzungsdefizite auftreten.

Eine Ad-hoc-Arbeitsgruppe „Versorgung im Einsatz“, die sich aus je zwei Teilnehmern aus den Bereichen BFA Bereitschaftspolizei, BFA Polizeiverwaltung und zwei Vorsitzenden der Haupt- / Gesamtpersonalräte in der Polizei zusammensetzte, ist auch in Vorbereitung auf künftige Einsätze dieser Art gezielt der Frage nachgegangen, woran es bei der Umsetzung des festgelegten Mindeststandards mangelt. Ferner wurden Empfehlungen erarbeitet, wie diese Mindeststandards umgesetzt werden können und welche Anforderungen an die Versorgung und die Unterbringung zu beachten sind.

4. Messen und Kongresse

4.1 Europäische Polizeikongresse des „Behörden Spiegel“

▸ 10. Europäischer Polizeikongress vom 3.–14. Februar 2010 in Berlin

Am 13. / 14. Februar 2007 fand im Berliner Congress Centrum (BCC) der 10. Europäische Polizeikongress statt. Schwerpunktthema des Kongresses war die Europäische Sicherheitsstrategie mit Fokus auf Konzepte und Technologien gegen Terrorismus. Veranstalter des Kongresses war der „Behörden Spiegel“. Teilnehmer waren Innen- und Justizminister auch aus Asien, Afrika und Europa, Staatssekretäre, Behördenleiter, Polizisten und Polizistinnen.

Die GdP präsentierte sich an einem Gemeinschaftsstand gemeinsam mit EuroCOP. Der Kongress wurde von GdP und EuroCOP auch dazu genutzt, auf die nationale und internationale Zusammenarbeit mit anderen Polizeigewerkschaften in Europa aufmerksam zu machen. Begleitet wurde der Kongress von Fachforen zur aktuellen Situation in der Polizei. In der Ausstellung der führenden Hersteller von Systemlösungen für die Sicherheitskräfte konnte man sich einen Überblick über das heute schon technisch Machbare verschaffen.

Der Bundesvorsitzende der GdP, Konrad Freiberg, war ein viel gefragter Interviewpartner diverser Medienvertreter. Außerdem moderierte er das Fachforum „Der Polizist der Zukunft".

11. Europäischer Polizeikongress am 29./30. Januar 2008 in Berlin

Der 11. Europäische Polizeikongress fand vom 29./30. Januar 2008 im Berliner Congress Centrum (BCC) statt.

Seit dem 9. Europäischen Polizeikongress war die GdP in Kooperation mit EuroCOP mit einem eigenen Stand vertreten.

Auf dem 10. Europäischen Polizeikongress wurde festgestellt, dass der Stand mit 9 qm zwischenzeitlich nicht mehr ausreichend war, um den Besuchern eine längere Verweildauer zu bieten.

Der „Behörden Spiegel" hat der GdP für den 11. Europäischen Polizeikongress eine größere Standfläche zur Verfügung gestellt. Aufgrund der vorgegebenen Baulichkeiten beträgt die Standfläche nun 36 qm.

Die GdP war auf dem 11. Europäischen Polizeikongress 2008 in Berlin nicht nur mit einem Stand vertreten. Der Bundesvorsitzende der GdP, Konrad Freiberg, und der Präsident von EuroCOP konnten jeweils als Redner im Hauptprogramm am ersten Tag der Veranstaltung platziert werden.

12. Europäischer Polizeikongress vom 10.–11. Februar 2009 in Berlin

Der 12. Europäische Polizeikongress fand unter dem Motto „Prävention: Prinzipien, Strategien, Technologien mit der gesamteuropäischen Zusammenarbeit und IT-Infrastruktur" statt.

13. Europäischer Polizeikongress vom 02.–03. Februar 2010 in Berlin

Der Kongress fand zum Thema „Globale Sicherheit – Herausforderungen für Europa" mit dem Schwerpunkt auf „Identität – Information – Infrastruktur" statt.

4.2 Moderner Staat

12. Fachmesse und Kongress Moderner Staat 2008

Anfang November 2008 fand ein weiterer Kongress „Moderner Staat" in Berlin statt, der durch eine Fachmesse begleitet wurde. Mit 3.620 Besucher und 213 ausstellenden Unternehmen unterstrich „Moderner Staat" 2008 erneut seine Position als bundesweit wichtigster Treffpunkt für die öffentliche Verwaltung.

Wie ein roter Faden zog sich der demografische Wandel als treibende Kraft für die künftige Entwicklung der öffentlichen Verwaltung bis ins Jahr 2020 hindurch. Er bringt tief greifende Änderungen für die öffentliche Infrastruktur und das Personal der Verwaltung mit sich: Das Potenzial der Erwerbspersonen wird aufgrund sinkender Geburtenzahlen abnehmen; die Mitarbeiter in der Verwaltung werden immer älter. 2007 war rund ein Viertel der Beschäftigten im höheren Dienst 55 Jahre und älter. Das Thema Führungskräfterekrutierung werde also verstärkt an Bedeutung gewinnen, so ein Referent. Lange unterschätzt worden sei auch das Thema Personalentwicklung als wichtiger Erfolgsfaktor. Neue Personalkonzepte würden nicht zuletzt darüber entscheiden, ob der öffentliche Dienst auch in Zukunft ein attraktiver Arbeitgeber bleibe.

Im Rahmen der Messe stellte die Prognos AG den Zukunftsreport „Moderner Staat" vor. Diese Studie beschreibt die wichtigsten Probleme und Handlungsfelder der öffentlichen Hand im Jahr 2020. Sie verdichtet die Prognosen und Vorstellungen ausgewählter Experten aus Verwaltung, Wirtschaft und Wissenschaft zur Zukunft der öffentlichen Verwaltung. Globalisierung und Europäisierung, moderne Technologien, neue Dialogformen, Demografie und Personalentwicklung und nicht zuletzt die Finanzsituation sind dabei wichtige Herausforderungen für die Zukunft (im Internet ist die Studie unter: „http://www.prognos.com" abrufbar).

Mehr als 200 Referenten und 100 Veranstaltungen wurden im Rahmenprogramm der Messe angeboten.

Allein der Kongress beleuchtete in insgesamt 31 Foren die aktuellen Entwicklungen, stellte Praxisbeispiele vor und gab konkrete Handlungsempfehlungen. Kongresspartner von „Moderner Staat" 2008 waren das BMI, die KGSt (Kommunale Gemeinschaftsstelle für Verwaltungsmanagement) und die DHV (Deutsche Hochschule für Verwaltungswissenschaften) Speyer.

Top-Themen auf „Moderner Staat" 2008 waren neben dem Projekt D115 (eine einheitlichen Behördenrufnummer) die Doppik (die Abkürzung steht für die DOPPelte Buchführung in Konten), Neuigkeiten aus den Projekten von Deutschland-Online sowie die Umsetzung der EU-Dienstleistungsrichtlinie.

Vom einheitlichen Ansprechpartner bis zu den technologischen Voraussetzungen – Die EU-Dienstleistungsrichtlinie berührt auch die Themenbereiche Personalmanagement und E-Government (Regieren und Verwalten mit Unterstützung von Informations- und Kommunikationstechniken).

Das Land Hessen, das in diesem Jahr offizielles Partnerland der Messe war, stelle den HessenPC vor. Dabei handelt es sich um einen landesweit einheitlichen Verwaltungsarbeitsplatz. Mit ihm hat Hessen die Plattform für eine einfache und einheitliche Bedienung von zentralen Verfahren geschaffen.

Ob demografischer Wandel, leistungsorientierte Bezahlung oder neue Fortbildungskultur – das Thema Personalmanagement bekam auch auf „Moderner Staat" eine immer größere Bedeutung. Wie sehr das Thema Personal die öffentliche Verwaltung in den nächsten Jahren fordern wird, zeigten neben zahlreichen Ausstellern auch die Referenten aus Verwaltung, Wissenschaft und Wirtschaft im Kongressprogramm.

13. Fachmesse und Kongress „Moderner Staat“ 2009

„Die Rolle des Staates in Zeiten des Umbruchs“ – so lautete das Motto der 13. Fachmesse und des Kongresses „Moderner Staat“ in diesem Jahr. Und als Erstes fragt man sich dabei: Welcher Umbruch ist da gemeint?

Vorweg: Das hat sich nicht so recht erschlossen. Dennoch haben vom 24. bis 25. November 2009 auf dem Messegelände in Berlin über 200 Aussteller auf rund 8.000 qm Ausstellungsfläche innovative Produkte und Dienstleistungen für die Verwaltungsmodernisierung präsentiert.

„Wir streben eine durchgreifende Modernisierung der Bundesverwaltung, einschließlich der Ministerien und nachgeordneten Behörden an“, so der Bundesinnenminister Dr. Thomas de Maizière in seiner Eröffnungsrede.

Es war Freiherr vom Stein, der den ganzen Staat schon einmal umgekrempelt, neue Verwaltungen geschaffen und versucht hat, dem Bürger zu seinem Recht zu verhelfen. Mit seinem Namen sind die Modernisierung der Verwaltung, die Bauernbefreiung, die Einführung der Wehrpflicht und die städtische Selbstverwaltung verbunden. Sein Motto: „Viel leisten, wenig hervortreten“. Er hatte „das verstaubte Preußen“ grundlegend reformiert und einmal gesagt: „Um eine Staatsverwaltung in tüchtigem Gange zu erhalten, müssten alle drei Jahre einige Minister, einige Generale und Dutzende Räte füsiliert werden – man müsste alle Beamten mit dem fünfzigsten Jahre wegjagen!“ So zitierte ihn auch der Bundesminister des Innern, Dr. Thomas de Maizière, MdB, in seiner Eröffnungsrede – bezog es allerdings auf die Politiker – und stellte das Verwaltungs-Programm für die nächsten Jahre klar:

> „Wir streben eine durchgreifende Modernisierung der Bundesverwaltung, einschließlich der Ministerien und nachgeordneten Behörden an. Das soll unter anderem durch eine umfassende Aufgabenkritik, die konsequente Standardisierung von Prozessen sowie durch weitere Entbürokratisierung geschehen. Wirkungen und Erfolge werden wir evaluieren und transparent kommunizieren. Neben dem Effizienzprogramm ist der Bürgerservice unser zweiter Schwerpunkt in den nächsten Jahren. Es ist ein zentrales Anliegen der Bundesregierung, Bürgernähe, Partizipation und Servicequalität der Bundesverwaltung weiter zu verbessern.“

Der Kongress befasste sich u. a. mit folgenden Themen:

Korruptionsbekämpfung in der öffentlichen Verwaltung – Lernen von der Privatwirtschaft?

Die Korruption ist in der öffentlichen Verwaltung schon seit geraumer Zeit Gegenstand wissenschaftlicher Analyse wie auch gesellschaftlicher Diskussion. Angesichts der durch Korruption verursachten Schäden ist es insbesondere die Frage nach Strategien und Maßnahmen zur Korruptionsbekämpfung, die im Fokus dieser Veranstaltung stand.

Projekt D115 – Einheitliche Behördenrufnummer im Pilotbetrieb

Seit das Projekt D115 – Einheitliche Behördenrufnummer – am 24. März 2009 in den Pilotbetrieb gestartet ist, haben rund 10 Millionen Bürger einen direkten Draht in die Verwaltung. Die 115 baut bürokratische Hürden ab und ist somit ein wichtiger Schritt zu einer bürgernahen Verwaltung.

Der Deutsche Städtetag, der Deutsche Landkreistag, der Deutsche Städte- und Gemeindebund und das Bundesministerium des Innern haben am ersten Kongress- und Messetag die „Gemeinsame Erklärung über die Zusammenarbeit im Rahmen des Projekts D115 – Einheitliche Behördenrufnummer“ unterzeichnet und bekennen sich damit zum weiteren Ausbau des Bürgerservice. Sie verpflichten sich, vertrauensvoll und kooperativ zusammenzuarbeiten, um eine deutschlandweite Verfügbarkeit der einheitlichen Behördenauskunft zu realisieren.

Auswirkungen der Finanzkrise auf die Kommunen

Die aktuelle Finanz- und Wirtschaftskrise beschert den Kommunen hohe Steuerausfälle, während die damit verbundenen Arbeitsmarktprobleme – vor allem bei einer länger anhaltenden Krise – zusätzliche Ausgaben für Langzeitarbeitslose nach sich ziehen. Die Konjunkturprogramme des Bundes fördern zwar ausgewählte kommunale Investitionen, erfordern aber einen Eigenanteil aus den kommunalen Haushalten. Diese Probleme treffen nicht nur strukturell gesunde Gemeinden und Gemeindeverbände, sondern auch solche mit sehr hohen, „chronischen“ Kassendefiziten in Regionen, in denen schon seit längerem ein dramatischer ökonomischer und demografischer Strukturwandel im Gang ist.

Personalmanagement im demografischen Wandel – Folgen und Vorsorge für die gesundheitliche Belastung von Mitarbeitern

Der demografische Wandel hat Auswirkungen auf die Altersstruktur der Beschäftigten in Betrieben, Verbänden und Verwaltungen: Die Gewinnung von Nachwuchskräften wird in Zukunft schwieriger.

Zugleich gehen die Beschäftigten später in den Ruhestand. Somit erhöht sich der Altersdurchschnitt der Belegschaften. Um die Beschäftigungsfähigkeit zu erhalten, spielt eine betriebliche Gesundheitsvorsorge für die Mitarbeiterinnen und Mitarbeiter eine immer wichtigere Rolle.

Dabei setzen Bund, Ländern, Kommunen und Verbänden am individuellen Bedarf an.

IT-Sicherheit zwischen Verfolgungswahn und Fahrlässigkeit

Aktuelle Angriffe, effektive Sicherheitsmaßnahmen und das Spannungsfeld zwischen Sicherheit und persönlicher Freiheit kennzeichnen diesen Bereich. Anhand der Live-Demonstration aktueller Angriffe gegen IT-Infrastrukturen wurde gezeigt, welchen Gefahren die öffentliche Verwaltung in der heutigen Informationsgesellschaft ausgesetzt ist. Kritisch wurden die Antworten des Gesetzgebers hinterfragt und Lösungsmöglichkeiten aufgezeigt.

Elektronische Identität und sichere Kommunikation im E-Government

Laut Statistischem Bundesamt waren 2007 knapp 70 % der Deutschen online. Einkaufen, tauschen und ersteigern, Online-Tagebücher und soziale Netzwerke gehören heute weitgehend zum Alltag. Doch für ein wesentliches Medium gibt es noch immer keine digitale Entsprechung: die Papierpost.

Unter dem Namen „De-Mail“ sollen Nachrichten und Dokumente daher ab 2010 zuverlässig und vor Veränderungen geschützt in einem sicheren Kommunikationsraum zwischen registrierten Nutzern versendet werden können.

De-Mail und das Bürgerportalgesetz schaffen die Rahmenbedingungen für den Aufbau einer Infrastruktur, die – ähnlich wie die Papierpost – für alle funktioniert:

Bürgerinnen und Bürger, Wirtschaft und Verwaltung können per De-Mail Nachrichten und Dokumente sicher elektronisch versenden und empfangen. De-Mail soll so einfach werden wie E-Mail und dabei so sicher und verbindlich wie die Papierpost. De-Mail und die zugehörigen Dienste erfüllen dabei die hohen Anforderungen an die Kommunikation zwischen Behörden und Bürgerinnen und Bürgern sowie der Wirtschaft.

Die 14. Fachmesse und Kongress „Moderner Staat“ finden vom 27. bis 28. Oktober 2010 auf dem Messegelände Berlin statt.

(Weitere Infos unter: www.modernerstaat.de)

4.3 Leitmesse für Polizei- und Spezialausrüstung (GPEC) 2008 in München

Seitens des Veranstalters der Leitmesse für Polizei- und Spezialausrüstung (GPEC), die in der Zeit vom 03. bis 05. Juni 2008 in München stattfand, lag eine Anfrage vor, ob sich die GdP mit einem Info-Stand an der Messe beteiligen möchte.

GPEC

Die GPEC General Police Equipment Exhibition & Conference ist eine geschlossene Spezialmesse für Polizeiausrüstung, Sicherheitstechnik und Dienstleistungen ausschließlich für Besucher aus Behörden. Ein spezielles Kongress- und Vortragsprogramm rundet die erstmals 2000 durchgeführte Veranstaltung ab. Sie findet alle zwei Jahre in Deutschland statt. Veranstalter ist die Exhibition & Marketing Wehrstedt GmbH.

Präsenz durch die VDP GmbH

In den zurückliegenden Jahren war die VDP GmbH mit einem Stand auf dieser Messe präsent. Für die GdP war ein Mitglied des BFA Bereitschaftspolizei als Repräsentant und Ansprechpartner an diesem Stand anwesend. Die VDP GmbH hat entschieden, an der GPEC 2008 in München nicht teilzunehmen.

Die GdP beteiligte sich, in Kooperation mit dem Landesbezirk Bayern, an der GPEC 2008 mit einem eigenen Info-Stand.

4.4 IPOMEX 2009 – Medienpartnerschaft mit der Halle Münsterland

Die Halle Münsterland GmbH hat als Ausrichter der IPOMEX 2009 der GdP den Entwurf eines Kooperationsvertrages vorgelegt und damit starkes Interesse bekundet, dass die GdP mit einem Info-Stand dort vertreten ist.

Der durch die Halle Münsterland GmbH vorgelegte Kooperationsvertrag basiert auf der gegenseitigen Erbringung bestimmter, festzulegender Leistungen.

Die IPOMEX fand vom 31.03. bis 02. April 2009 zum vierten Mal als Polizeifachmesse in der Halle Münsterland statt.

Die GdP beteiligte sich an der IPOMEX 2009 mit einem Info-Stand.

Bericht über die IPOMEX 2009

Es war die 4. Internationale Polizeifachmesse IPOMEX, bei der auch die Gewerkschaft der Polizei Präsenz zeigte. Im Rahmen einer Medienpartnerschaft mit dem Veranstalter war die GdP mit einem Info-Stand präsent, der von vielen GdP-Mitgliedern auch als Anlaufstelle genutzt wurde.

Die Erwartungen des Veranstalters, des Messe und Congress Centrums Halle Münsterland, wurden weit übertroffen.

Offiziell wurde die dreitägige Messe am 31. März 2009 durch deren Schirmherrn und nordrhein-westfälischen Innenminister Dr. Ingo Wolf eröffnet. Insgesamt konnte der Veranstalter mehr als 4.200 Fachbesucher aus Behörden und Organisationen mit Sicherheitsaufgaben sowie der Bundeswehr verzeichnen.

Über 100 Aussteller boten einen Überblick über die technischen Neuheiten. Begleitet wurde die Messe von einem umfangreichen Rahmenprogramm aus Fachkonferenzen, Workshops, Vorträgen und auch zahlreichen Vorführungen, auch im Freigelände der Messe.

Polizei-Teams aus Köln und Bonn führten z. B. vor, wie sich die Qualität der Verkehrsunfallaufnahme verbessert hat.

Abschließend bleibt festzustellen, dass sich die IPOMEX als Fachmesse von Praktikern für Praktiker aus Behörden und Organisationen mit Sicherheitsaufgaben etabliert hat.

Die 5. IPOMEX findet in der Zeit vom 12. bis 14. April 2011 wieder in Münster statt. (www.ipomex.de)

4.5 Polizeitage 2010

Kooperation mit dem „Behörden Spiegel“; Gemeinsame Veranstaltungen 2010

Der „Behörden Spiegel“ hatte bereits im Jahr 2008 das Ansinnen geäußert, mit der GdP gemeinsam Veranstaltungen durchführen zu wollen. Bis dato war jedoch u. a. die Kostenfrage nicht eindeutig geklärt.

Der „Behörden Spiegel“ teilte der GdP mit, dass mit den gemeinsamen Veranstaltungen im Frühjahr 2010 begonnen werden könnte. Dabei wurde an „Tagesseminare“ gedacht, die z. B. unter dem Thema „Gewalt – die gegenwärtige Herausforderung“ oder aber „Internetkriminalität“ in vier Städten stattfinden sollten.

Das finanzielle Konzept sah so aus, dass der „Behörden Spiegel“ das finanzielle Risiko trägt und die Tagungen über Teilnehmergebühren und Sponsorengelder refinanziert würden. GdP-Mitglieder sollen freien Zutritt zu den Veranstaltungen haben, die übrigen Besucher mussten eine Tagungspauschale entrichten.

Mit der Bewerbung der Veranstaltung wurde auf dem 13. Europäischen Polizeikongress, Anfang Februar 2010, begonnen und im „Behörden Spiegel“ fortgesetzt. Auch in Deutsche Polizei und auf der Homerpage der GdP wurden die Veranstaltungen beworben. Ferner unter: www.polizeitage.de

Die Veranstaltungen wurden im März 2010 begonnen,

Die geplanten und gemeinsam durchgeführten Veranstaltungen wurden inhaltlich und terminlich in enger Absprache mit den jeweiligen Landesbezirksvorsitzenden festgelegt.

Die organisatorischen Vorbereitungen erfolgten durch den „Behörden Spiegel" bzw. den ProPress Verlag in Bonn.

Die Veranstaltungen sollten wie folgt stattfinden:

11./12.03.2010 Hamburg
Gewalt – eine zunehmende Herausforderung für Politik, Polizei und Gesellschaft

07./08.06.2010 München
Gewalt – eine zunehmende Herausforderung für Politik, Polizei und Gesellschaft

08./09.07.2010 Düsseldorf
Polizei der Zukunft – Zukunft der Polizei

12./13.07.2010 Hannover
Cybercrime, Cyberware, Cyberdefence (angefragt)

01./02.09.2010 Berlin
Abschlussveranstaltung (noch ohne Titel)

5. Dokumentationsstelle

Die Bibliothek und Dokumentationsstelle der Gewerkschaft der Polizei stellt Fachinformationen aller Art für die Arbeit der Bundesgeschäftsstelle und der Wirtschaftsunternehmen, für die GdP-Landesbezirke und Bezirke, für Funktionsträger in den GdP-Gremien bundesweit. Letztlich profitiert jedes einzelne GdP-Mitglied von den Serviceleistungen der Dokumentationsstelle, wobei insbesondere die jüngeren Kolleginnen und Kollegen in der Ausbildung diese Dienstleistungen zu schätzen wissen. Ziel ist die Unterstützung der gewerkschaftspolitischen und polizeilichen Arbeit.

In der Dokumentationsstelle werden Fachliteratur, Rechtsprechung und Beschlusslagen der GdP gesammelt, aufbereitet und erschlossen, um anhand dieser Materialien die Informationsvermittlung für die Nutzerinnen und Nutzer bestmöglich zu gestalten.

Neben der Nutzung der klassischen, gedruckten Bibliotheksbestände setzt die Dokumentationsstelle verstärkt auf den Einsatz neuer Medien. Hierzu gehören professionelle Internet-Recherchen ebenso wie die Nutzung von Datenbanken anderer Institutionen und gewerblicher Datenbankanbieter.

Derzeit verfügt die Dokumentationsstelle über einen Buch- und Zeitschriftenbestand von ca. 10.000 Bänden sowie 230 laufenden Abonnements (Zeitschriften und Loseblattwerke). Schwerpunkte des Bestandes bilden die Themenbereiche Recht, Politik, Polizei und Kriminalistik sowie gewerkschaftlich relevanten Themen.

Der bereits in den 80er Jahren begonnene Aufbau einer Datenbank (ehemals ROMULUS) wurde mit dem Einsatz einer neuen Bibliothekssoftware (WinBIAP.net der Firma datronic, Augsburg) seit 2005 auf eine moderne Ebene gehoben und umstrukturiert. Mit der Umstrukturierung hin zu einer Literaturdatenbank war die Vision verbunden, langfristig alle GdP-Mitglieder an diesem Fundus teilhaben zu lassen.

Diese Literaturdatenbank dient als Fundstellennachweis für Bücher und Fachaufsätze, die in der Bibliothek und Dokumentationsstelle der GdP Bundesgeschäftsstelle vorhanden sind. Derzeit sind in ihr mehr als 31.000 Fundstellennachweise gespeichert, davon mehr als 23.000 Fachaufsätze. Diese Daten können nicht nur durch formale Kriterien (z. B. Autor oder Titel) abgefragt werden, sondern werden darüber hinaus nach inhaltlichen Kriterien (z. B. Schlagwörter oder Annotationen) erschlossen und erleichtern damit die Literatursuche für Gewerkschaftsbeschäftigte und Mitglieder in erheblichem Maße. Die besondere Ausrichtung der Sammlung und deren Aktualität – jährlich kommen ca. 2.500 Datensätze neu hinzu – machen sie zu einer einzigartigen Hilfestellung für die beruflichen und gewerkschaftlichen Zwecke unserer GdP.

Im Mai 2008 konnte dieses Ziel erreicht werden. Erstmals war es allen Gewerkschaftsmitgliedern der GdP möglich, im internen Mitgliederbereich des GdP-Webauftritts in der Literaturdatenbank selbstständig zu recherchieren.

Mit zwei Artikeln in DEUTSCHE POLIZEI (Ausgabe 4/2008 und 9/2009) wurde die GdP-Literaturdatenbank als neuer Mitgliederservice vorgestellt. Für Werbezwecke wurde ein Flyer produziert, der der Juni-Ausgabe 2008 DEUTSCHE POLIZEI beigelegt war (siehe Anlage 4).

Die GdP ist die einzige Polizeigewerkschaft mit einem solchen Angebot. Grund genug für Landesbezirke und Bezirke, den Flyer und das damit verbundene, exklusive Serviceangebot der Bundesgeschäftsstelle zur Mitgliederwerbung und zum Ausbau der Mitgliederbetreuung zu nutzen.

Die Resonanz bei den (Neu-)Mitgliedern ist durchweg sehr positiv und das Serviceangebot wird so gut angenommen, dass die beiden Kolleginnen der Dokumentationsstelle die zunehmende Nachfrage in diesem Bereich kaum noch bewältigen können.

Damit bestätigt sich, dass die Konzeptentwicklung der GdP-Literaturdatenbank von einer internen Dienstleistung der Dokumentationsstelle über einen Service für die Landesbezirke und Bezirke bis hin zu einem festen Serviceangebot der Bundesgeschäftsstelle für alle GdP-Mitglieder ein Erfolg ist.

Die Dokumentationsstelle der GdP hat sich landesweit den Ruf erworben, schnell und kompetent benötigte Informationen an die Frau bzw. an den Mann zu bringen. Die Literaturdatenbank ist dabei ein Baustein von vielen.

6. PC-Anwenderservice

In der heutigen Zeit ist ein Büroarbeitsplatz ohne PC kaum mehr vorstellbar, erleichtert und beschleunigt er doch spürbar viele Arbeitsabläufe und sorgt für schnelle Kommunikation. Doch kein Programm läuft dauerhaft fehlerfrei, kein Gerät ist störunanfällig, und keine Software ist so schlau, dass sie alle Bedienungsfehler abfängt. Regelmäßig ändern sich die Anforderungen, welche Daten wie erfasst, verarbeitet und vor allem archiviert werden. Die Situation der Anwender und ihre Beratung ist kritisches Potenzial für Erfolg und Misserfolg des Einsatzes neuer Hard- und Software.

Der hohe Ausstattungsgrad der GdP-Bundesgeschäftsstelle mit vernetzten IT-Systemen sowie die wachsende Komplexität der eingesetzten Anwendungsprogramme erfordern eine umfassende fach- und sachkundige Betreuung der Anwendungen und der Anwender, um das Funktionieren der

Hard- und Software zu gewährleisten und den größtmöglichen Nutzen aus den vorhandenen Anwendungen zu erzielen. Eine solch umfassende und sorgfältige Betreuung stellt nicht nur die Voraussetzung für die Akzeptanz technischer Innovationen durch die Anwender dar, sondern ermöglicht auch ein weitestgehend störungsfreies, effektives Arbeiten.

Der PC-Anwenderservice ist Ansprechpartner für alle Anwenderinnen und Anwender der GdP-Bundesgeschäftsstelle sowie die Mitglieder des GBV und auf Anfrage teilweise auch der Landesbezirke für sämtliche Fragen und Probleme rund um die Hard- und Software. Er ist zudem ein Bindeglied zwischen den Anwendern der GdP-Bundesgeschäftsstelle und der EDV-Abteilung der Organisations- und Service-Gesellschaft der Gewerkschaft der Polizei mbH (OSG). Anfragen und Probleme der Anwender werden vom PC-Anwenderservice entgegengenommen und persönlich vor Ort oder via Fernwartung gelöst oder entsprechend den Zuständigkeiten an die OSG oder Externe weitergeleitet.

Zum Aufgabengebiet des PC-Anwenderservice gehören:

- Administration und Pflege des elektronischen Archivs ELO
- Einzelfallbezogene Unterstützung der Anwender bei der Bedienung der Anwendungsprogramme und der eingesetzten Geräte
- Umgehende bzw. zeitnahe Fehlerdiagnose und -behebung von Anwender- und Anwendungsfehlern sowie Hardwareausfällen
- Unterweisung von Anwendern und Einweisung neuer Mitarbeiter in die Programmbedienung
- Beratung der Anwender bei der DV-technischen Unterstützung der Arbeitsabläufe sowie in Ausstattungs- und Ergonomiefragen
- Eigene Umsetzung bzw. Formulierung und Weiterleitung von Programmanforderungen an die Entwickler (z. B. GdP-spezifische Anpassungen in ELO)
- Installation von Hard- und Software und deren Anpassung an die individuellen Bedarfe
- Erstellung von Step-by-Step-Anleitungen für die Anwender intern sowie bei Bedarf auch für externe Kolleginnen und Kollegen
- Organisatorische und inhaltliche Vorbereitung externer Schulungen, beratende und vermittelnde Teilnahme daran (ergänzend zur Herstellerfirma bezüglich des GdP-spezifischen Einsatzes an den Arbeitsplätzen)
- Vorbereitung und Durchführung von eigenen Schulungen und Workshops und deren Nachbereitung
- Erstellung von Präsentationen, komplexeren Layouts (z. B. erste Ausgaben des Newsletters der Frauengruppe Bund) und kleineren Access-Datenbanken entsprechend den Wünschen der einzelnen Abteilungen bzw. GBV-Mitgliedern
- Erstellung von Formularen, Dokumentvorlagen etc.
- Teilnahme an den Sitzungen der ELO-Arbeitsgruppe (Abt. I) und der Kommission Systemsicherheit

Das Aufgabengebiet des PC-Anwenderservice GdP ist vielfältig, der alltägliche Umgang mit der EDV wirft häufig zeitlich unplanbare Fragen und Problemstellungen unterschiedlicher Art auf. Im Folgenden daher nur ein Überblick über die größeren Projekte im Berichtszeitraum.

Dokumentenmanagement-System der GdP-Bundesgeschäftsstelle ELO

Ende 2005 wurden in der Bundesgeschäftsstelle Berlin und Hilden das Dokumentenmanagement-System (DMS) ELO sowie die dafür erforderliche Hardware (leistungsfähige Rechner, schnelle Scanner usw.) eingeführt. Die Leitung für das Projekt ELO liegt bei der Geschäftsführung. Das gesamte Projekt wurde inhaltlich und organisatorisch aktiv vom PC-Anwenderservice begleitet.

Bis zur Einführung des elektronischen Archivs ELO wurde in der GdP-Bundesgeschäftsstelle an vielen unterschiedlichen Orten abgelegt. Es gab zum einen die unzähligen Aktenordner in Schränken und im Archivkeller, die digitale Ablage im Netzwerk oder auf der Festplatte der im PC erstellten Dokumente, die Ablage der E-Mails im Mailprogramm usw. Jede Abteilung legte nach eigenem System ab. Hinzu kam, dass Vorgänge aufgrund unterschiedlicher Zuständigkeiten jeweils in mehreren Abteilungen gesammelt wurden. War somit die Ablage schon mühsam, so gestaltete sich die Suche nach bestimmten Vorgängen zeitaufwändig und manches Mal auch erfolglos.

Nach intensiver Vorbereitung durch die Arbeitsgruppe ELO sowie in Zusammenarbeit mit der Augsburger Firma Holme & Co, Spezialist für Archivierungs- und Dokumentenmanagement-Lösungen, beschloss der GBV in seiner Sitzung im Juni 2005 die Anschaffung von ELO für die GdP-Bundesgeschäftsstelle.

Zielsetzungen bei der Einführung von ELO waren u. a. die weitestgehend papierlose Ablage, Vermeidung von Mehrfachablagen sowie die schnelle und abteilungsübergreifende Verfügbarkeit von Informationen jeglicher Art und Herkunft. Dokumente, E-Mails, Mediendateien, Internetlinks u. v. m., sowohl in Papierform als auch digital vorliegend, werden in ELO erfasst, verwaltet und bereitgestellt und sind durch die integrierten Suchmechanismen des Programms schnell auffindbar. Dateien und Dokumente können in anzeigefähigen Langzeitformaten umgewandelt und archiviert werden. Damit ist sichergestellt, dass die Dokumente auch nach vielen Jahren noch lesbar sind. Um einen Informationsgleichstand zwischen den Bundesgeschäftsstellen Hilden und Berlin zu gewährleisten, werden die Daten in kurzen Zeitabständen repliziert.

Gleichzeitig mit der Einführung von ELO wurden die in der GdP-Bundesgeschäftsstelle eingesetzten Notebooks mit ELO Mobil ausgestattet. Mit dieser Funktionalität stehen den Kolleginnen und Kollegen auch unterwegs alle für sie relevanten Dokumente und Informationen zur Verfügung. Zurück im Büro werden die Daten von Hauptarchiv und Mobil abgeglichen und auf beiden Seiten aktualisiert.

Um auch den Mitgliedern des Geschäftsführenden Bundesvorstandes der GdP einen schnellen und plattformunabhängigen Zugriff auf die Dokumente der GdP-Bundesgeschäftsstelle zu ermöglichen, wurden im Oktober 2006 Lizenzen für

das ELO Internet Gateway erworben. Damit können die Mitglieder des GBV über einen Internetbrowser auf den aktuellen Datenbestand des ELO-Archivs der GdP-Bundesgeschäftsstelle zugreifen. Damit das Programm effektiv genutzt werden kann, wurde vom PC-Anwenderservice eine Schulung durch die Firma Holme für die Mitglieder des GBV organisiert. Spätere Einzel- bzw. Nachschulungen wurden und werden vom PC-Anwenderservice durchgeführt.

Mit der Einführung von ELO wurde der PC-Anwenderservice mit der Administration und Pflege dieses Systems beauftragt. Dies stellt daher seit Ende 2005 einen weiteren Aufgabenschwerpunkt des PC-Anwenderservice dar. Zu diesen Aufgaben gehören u. a.:

- Benutzerverwaltung
  (Neueinrichtung, Rechtevergabe, Replikationszuordnungen, Gruppenzuordnungen etc.)
- Erstellung GdP-spezifischer Ablagemasken,
  Stichwortlisten etc. und deren Verwaltung und Pflege
- Festlegung von ELO-Optionen für alle Anwender und einzelplatzbezogen
- Teilnahme an Arbeitsgruppen sowie Vorbereitung und Durchführung von Workshops zur Weiterentwicklung des Systems
- Fertigen von Fehlerbeschreibungen und Verbesserungsvorschlägen und Weiterleitung an Firma Holme
- Erstellung von Kurzanleitungen für die Anwender bezüglich GdP-spezifischer Besonderheiten bzw. Veränderungen des Programms
- Kontrolle der ELO-Dienste
- Überwachung der Replikation Broker/Branch zwischen Hilden und Berlin
- Administration und Pflege der ELO-Profil-Datenbank in Lotus Notes

Obwohl ELO bereits seit fünf Jahren im Echtbetrieb ist, zeigt sich, dass aufgrund der Komplexität der Software immer wieder kleinere oder auch größere Probleme im Alltag auftreten, die eine schnelle Hilfestellung erforderlich machen, um einen ungestörten weiteren Bearbeitungsfluss zu ermöglichen und bestehende Unsicherheiten im Umgang mit der Software zeitnah zu beheben. Zudem müssen – da es sich bei keiner Software um ein „fertiges" Produkt handelt oder auch Aufgabenstellungen sich ändern – immer wieder aktuelle Anpassungen auf Administratorebene vorgenommen werden. Die Erfüllung dieses Aufgabenbereiches erfordert vom PC-Anwenderservice nach wie vor große zeitliche Ressourcen.

Seit der Einführung von ELO bis Ende April 2010 wurden von allen Abteilungen der Bundesgeschäftsstelle Hilden und Berlin insgesamt ca. 122.000 Dokumente in diesem elektronischen Archiv abgelegt.

Anschaffung und Installation neuer Monitore

Nach der Einführung von ELO nahmen die Arbeiten sowie das Lesen auch sehr langer Texte am Bildschirm um ein Vielfaches zu. Zum damaligen Zeitpunkt standen sowohl an den Arbeitsplätzen in Hilden als auch in Berlin unterschiedliche Monitormodelle, überwiegend in der Größe 17 Zoll. Aus arbeitsergonomischer Sicht war besonders negativ zu bewerten, dass die meisten dieser Monitore weder höhen- noch neigungsverstellbar waren.

Um auch aus ergonomischer Sicht den mit der Einführung von ELO verbundenen veränderten Arbeitsabläufen gerecht zu werden, regte der PC-Anwenderservice Anfang 2007 eine Neuanschaffung größerer und vor allem durchgängig höhen- und neigungsverstellbarer Monitore an den Arbeitsplätzen der Bundesgeschäftsstelle an. Mitte 2007 wurde die Entscheidung über die Neuanschaffung entsprechender Monitore getroffen. Nach ausführlicher Recherche und intensiven Tests mit unterschiedlichen Monitormodellen verschiedener Hersteller fiel Ende 2007 die Wahl auf ein21-Zoll-Modell, das alle geforderten Kriterien erfüllte. Dieses wurde nach Rücksprache mit dem zuständigen GBV-Mitglied durch den PC-Anwenderservice für alle Arbeitsplätze der Bundesgeschäftsstelle beschafft.

Ausstattung der GdP-Bundesgeschäftsstelle mit neuer Hard- und Software

Im März 2010 wurde die GdP-Bundesgeschäftsstelle mit neuen Desktop-PCs und Notebooks sowie aktueller Software (Betriebssystem Windows 7, Office 2007, Lotus Notes 8.5, ELO Professional 7.0) ausgestattet. Die vorbereitenden Arbeiten an den Arbeitsplätzen (Sicherung von Anwenderdaten und benutzerspezifischer Einstellungen), Terminkoordinierung für das Gesamtprojekt, die Organisation, inhaltliche Vorbereitung und Begleitung der externen Schulungen in den oben genannten Programmen (außer Lotus Notes) wurden vom PC-Anwenderservice durchgeführt.

Des Weiteren wurden in enger Zusammenarbeit mit der Augsburger Firma Holme & Co, Spezialist für Archivierungs- und Dokumentenmanagement-Lösungen, die Vorbereitungen für die Umstellung auf die neue ELO Professional Version 7.0 getroffen. Ein ausführliches Gespräch zu Planung, Umfang und Abwicklung der ELO-Umstellung fand Anfang Februar 2010 zwischen der GdP-Geschäftsführung, dem PC-Anwenderservice und der Firma Holme & Co in Augsburg statt.

Die Installation der Hard- sowie der Standardsoftware erfolgte durch die EDV-Abteilung der OSG.

Die Rücksicherung der Anwenderdaten, die Anpassung der einzelnen Arbeitsplätze auf die individuellen Bedarfe der Anwender, die Installation von Peripheriegeräten und benutzerspezifischer Software sowie die Installation von ELO sowohl auf den Arbeitsplatz-PCs als auch auf der Vielzahl der Notebooks erfolgten durch den PC-Anwenderservice; alle serverseitigen Arbeiten betreffend ELO wurden von der Firma Holme & Co abgewickelt.

7. Sonstiges

7.1 Leitung der Geschäftsstelle Hilden

Zum Aufgabengebiet der Abt. IX gehört auch die Leitung der Geschäftsstelle Hilden. Neben den organisatorisch-administrativen Tätigkeiten wie Pflege der Arbeitszeitkonten der in der Geschäftsstelle beschäftigten Mitarbeiterinnen und Mitarbeiter, der Genehmigung und Verwaltung von Urlaubsanträgen usw. gehören dazu auch das Wahrnehmen von kleinen und großen Probleme, die im Arbeitsleben auftreten, seien sie fachlicher, sachlicher oder personeller Art, das Weiterleiten von Informationen unterschiedlichster Herkunft, die für die Beschäftigten von Interesse sind, u. v. m. Die Leitung erfolgt in enger Abstimmung mit der Geschäftsführung der GdP in Berlin.

7.2 Digitalisierung der Bundes-Gremien-Protokolle der GdP

Zwischenzeitlich konnten über eine Firma, die sich auf die Digitalisierung von Akten und Büchern spezialisiert hat, alle GdP-Bundes-Gremien-Protokolle von 1951 bis 1996, die als gedruckte und gebundene Werke vorlagen, digitalisiert werden.

Sie liegen nun im PDF-Format vor und nehmen ein Gesamtvolumen von circa 20 Gigabyte ein.