Die Phänomenologie der IuK-Kriminalität reicht von der missbräuchlichen Verwendung von Telekommunikationsanlagen (sog. „Phreaking“) bis hin zu den bisher hypothetischen Bedrohungsszenarien, die durch Angriffe auf kritische Infrastrukturen (sog. „Cyber-Terrorismus“) entstehen können. Daneben bietet das Internet im Rahmen des e-commerce eine willkommene Plattform der verschiedensten Betrugsformen. Durch die möglich gewordenen neuen digitalisierten Begehungsweisen des klassischen Deliktspektrums bereitet das Internet als „Nervensystem“ der modernen Dienstleistungsgesellschaft der Strafverfolgung enorme Probleme.

So wurde denn auch auf der Herbsttagung 2003 des Bundeskriminalamtes der Bogen von der „schönen neuen Welt“ bis hin zu den „Schattenseiten“ des modernen Mediums gespannt. Die Fragestellung, ob rechtsfreie Räume in einem gewissen Umfang zugelassen werden, die Anarchie im Netz also akzeptiert wird, zeigt das Spannungsfeld zwischen Strafverfolgung und Wirtschaft auf. Dieser Herausforderung muss sich die Strafverfolgung zukünftig stellen. Klassische Denkmuster und hergebrachte Methoden müssen einem neuen Instrumentarium weichen, das den neuen Bedingungen gerecht wird. Auch wenn das Internet der Strafverfolgung technische und tatsächliche Grenzen setzt, darf dies nicht heißen, das Feld zu Lasten der Sicherheit der Bürger preis zu geben.

Dass dies nur in einem umfassenden und vorbehaltlosen Dialog aller Gesellschaftsschichten erfolgreich sein kann, wurde auf der BKA-Tagung deutlich.

ISBN: 3-472-06108-1
9 783472 061083

www.luchterhand-fachverlag.de

Informations- und Kommunikationskriminalität

Bundeskriminalamt

Informations- und Kommunikations-kriminalität

BKA-Herbsttagung 2003

Luchterhand

Informations- und Kommunikationskriminalität

Polizei + Forschung
Bd. 27
herausgegeben vom
Bundeskriminalamt (BKA)
Kriminalistisches Institut

Bundeskriminalamt

Bundeskriminalamt (Hg.)

Informations- und Kommunikations-kriminalität

Vorträge anlässlich der Herbsttagung des Bundeskriminalamtes vom 2. bis 4. Dezember 2003

BKA

Luchterhand

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Redaktion:

Heinrich Schielke

Bundeskriminalamt
Kriminalistisches Institut

Umschlaggestaltung: arttec grafik simon & wagner, St. Goar
Satz: Satz Offizin Hümmer, Waldbüttelbrunn
Druck: Druckerei Wilhelm & Adam, Heusenstamm
Printed in Germany, Dezember 2004

♾ Gedruckt auf säurefreiem, alterungsbeständigem und chlorfreiem Papier

Inhaltsverzeichnis

Begrüßung

Ulrich Kersten

Sehr verehrter Herr Minister, sehr geehrter Herr Professor Glotz, sehr geehrte Frau Abgeordnete, meine Herren Abgeordneten, meine sehr verehrten Damen und Herren, liebe Kolleginnen und Kollegen,

zur diesjährigen Arbeitstagung des Bundeskriminalamts heiße ich Sie ganz herzlich willkommen. Es ist nunmehr die 49. Tagung, die das BKA jährlich im Herbst ausrichtet. Wir sind überzeugt, dass auch das diesjährige Arbeitsthema Ihre Zustimmung und Aufmerksamkeit finden wird. Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnologien – ein relativ junges Kriminalitätsphänomen und doch aufgrund der Dynamik, die in der Entwicklung dieses Technologiefeldes zu konstatieren ist, ein äußerst aktuelles Thema, das allemal unserer besonderen Aufmerksamkeit bedarf. Sei es unter dem Gesichtspunkt der Prävention, auch in Zusammenarbeit mit der Wirtschaft, der Strafverfolgung, der internationalen Zusammenarbeit, der Gesetzgebung oder der Forschung und Methodenentwicklung.

Die Bundesrepublik Deutschland hat, wie viele andere Länder auch, in der Entwicklung längst den Schritt hin zu einer modernen Informationsgesellschaft vollzogen. Die rasch fortschreitende Verbreitung digitaler Informations- und Kommunikationstechnologien durchdringt nahezu alle Lebensbereiche und verändert – wer will es bestreiten – zunehmend unseren Alltag. Seit der allgemeinen Öffnung des Worldwide Web hat sich das Internet in schier unglaublichem Tempo zum bedeutendsten Massenmedium entwickelt. Ohne damit den Spitzenplatz weltweit einzunehmen, verfügen bereits heute rund 43 % der deutschen Haushalte über einen Internetanschluss. 71 % der Unternehmen befragter Wirtschaftszweige setzten im Jahre 2002 Computer im Geschäftsablauf ein. Die Zahl der Internetnutzer weltweit wird auf über 700.000.000 geschätzt mit steigender Tendenz. Wirtschafts- und Produktionsprozesse, Steuerung von Versorgungseinrichtungen, Verwaltungsabläufe und privater Nachrichtenverkehr werden zunehmend unter Einsatz von neuen Informations- und Kommunikationstechnologien bewältigt.

Ich denke, es ist nicht übertrieben, diese Technologien inzwischen als Nervensystem der modernen Industrie- und Dienstleistungsgesellschaften zu bezeichnen. Viele behaupten, der Ausbau der Informationsgesellschaft befinde sich noch in einem Anfangsstadium. Und wie nicht anders zu erwarten, werden mit dieser Einschätzung Chancen und Risiken zugleich verbunden. Zu diesem Thema werden Sie, verehrter Herr Professor Glotz, uns in Ihrem Festvortrag Ihre Sicht der Zukunft vermitteln. Ich darf Sie ganz herzlich in unserer Mitte begrüßen.

Die Potenziale, die in den neuen Technologien stecken, gereichen nicht nur gesellschaftlichen und wirtschaftlichen Abläufen zum Vorteil. Leider machen

sich auch Straftäter die technischen Möglichkeiten zu Nutze, indem sie die Technologie als Tatmittel verwenden oder zum Tatobjekt beziehungsweise Tatziel machen. Unabhängig davon, meine Damen und Herren, dass sich Straftäter über Planung und Vorbereitung von Straftaten unter Verwendung moderner Kommunikationsmittel austauschen, ihren Finanzbereich durch neue Technik steuern und kriminell erworbene Gelder waschen, nutzen sie etwa das Internet, um strafrechtlich relevante Informationen zu verbreiten, wobei wir einem breiten Spektrum von Kriminalitätsfeldern begegnen. Ich nenne ohne Anspruch auf Vollständigkeit Kinderpornographie, extremistische Propagandadelikte, Anleitung zur Herstellung von Drogen oder Sprengsätzen.

Dr. Ulrich Kersten, Präsident des Bundeskriminalamtes, begrüßte die Tagungsteilnehmer

Ebenso begegnet uns der Tatort Internet bei der zu beobachtenden Zunahme betrügerischer Handlungen im Zusammenhang mit E-Commerce oder Online-Auktionen. Wirtschaftskriminalität, Urheberrechtsverletzung, Erpressung und Hehlerei runden das Bild ab. Auch wenn es sich hierbei im Grunde nicht um eigentlich neue Kriminalitätsfelder handelt, sondern Tatbegehungsweisen lediglich digitalisiert werden, so haben sich doch durch die Nutzung der neuen Technologien Qualität und Quantität des Täterverhaltens und der Tatfolgen erheblich verändert. Das Eindringen in digitale Telefonnetze oder in elektronische Zahlungsabläufe wie etwa beim Online-Banking mit dem Ziel, sich Vermögenswerte zu Lasten Dritter rechtswidrig zu verschaffen, können wir leider nicht nur als Fiktion abtun.

Die polizeiliche Kriminalstatistik erfasst für das Jahr 2002 ca. 57.000 Fälle der Computerkriminalität. Der dabei polizeilich registrierte Schaden beläuft sich

auf etwa 85.000.000 €. Meine Damen und Herren, nicht eingerechnet in diese Summe sind Schäden, die durch Angriffe auf Informations- und Kommunikationsstrukturen oder Eingriffe mit dem Ziel der Veränderung oder Vernichtung von Datenbeständen verursacht werden. Etwa durch Installation und Versenden von Trojanern, Viren und Würmern – aus welchen Motiven und durch wen auch immer dies geschieht. Man muss heutzutage offensichtlich kein ausgemachter Computerexperte sein, um solche Programme zu entwickeln und einzusetzen. Die dadurch entstandenen Schäden sind weitgehend nicht quantifizierbar. Immerhin, die Computerfachzeitschrift Chip schätzt in ihrer letzten Ausgabe vom November des Jahres die durch Viren, Würmer und Trojaner weltweit verursachten Folgeschäden auf einen zweistelligen Milliardenbetrag. Betroffen sind flächendeckend Unternehmen, öffentliche Verwaltungen und private Haushalte.

Meine Damen und Herren, Polizei und Justiz werden bei der Aufdeckung, Aufklärung und Verfolgung von Kriminalität im Zusammenhang mit der Informations- und Kommunikationstechnologie vor erhebliche Probleme gestellt. Stichworte hierfür mögen sein: Die Komplexität der Materie, schwer zu erfassende und für viele ggf. auch schwer zu begreifende technische Abläufe, Flüchtigkeit der Daten, Verfügbarkeit von Verschlüsselungstechnik, beides im Übrigen mit Folgen für die Beweissicherung, notwendige Zusammenarbeit mit Providern und nicht zuletzt ein umfang- und detailreiches gesetzliches Regelungswerk. Wir wollen diesen Fragen der Praxis in unserer Tagung Raum geben.

Ich freue mich daher, dass auch dieses Mal Vertreter von Polizei und Justiz in großer Zahl unserer Einladung gefolgt sind. Ich darf Sie, meine Damen und Herren, herzlich begrüßen und bitte um Nachsicht, dass ich nicht alle namentlich hier nenne.

Die Aufdeckung und die Aufklärung von Straftaten des Phänomenbereichs gestaltet sich auch deshalb schwierig, weil die virtuellen Netze weltweit ausgelegt sind und es den Tätern ermöglichen, ohne Schwierigkeiten grenzüberschreitend von Kontinent zu Kontinent zu agieren. Demgegenüber sind der staatenübergreifenden Zusammenarbeit der Strafverfolgungsbehörden trotz allen Engagements und trotz aller inzwischen erreichten Fortschritte in der internationalen Zusammenarbeit noch Grenzen tatsächlicher und rechtlicher Natur gesetzt. Möglichkeiten für etwaige Optimierungen auf diesem Feld aufzuzeigen ist auch ein Ziel unserer Tagung. Ich freue mich daher, dass Vertreter ausländischer Polizei- und Justizbehörden den Weg ins Bundeskriminalamt gefunden haben, um mit uns in einen Gedankenaustausch einzutreten. Meine Damen und Herren, ich darf Sie ganz herzlich begrüßen.

Das wirksamste Mittel, sich vor Angriffen gegen Strukturen der Informations- und Kommunikationstechnologie, insbesondere der kritischen Infrastrukturen zu schützen, ist die Prävention. Dies ist der gesetzliche Auftrag des Bundesamts für die Sicherheit in der Informationstechnik, dessen Präsidenten, Herrn Dr. Helmbrecht, ich ganz herzlich begrüße. Herr Dr. Helmbrecht, Sie werden uns

über die Aktivitäten und die Initiativen Ihres Hauses, in die auch das Bundeskriminalamt in vielfältiger Weise eingebunden ist, berichten.

Meine Damen und Herren, aus dem Bereich des Sports ist das Wortspiel bekannt: Wer nicht mitläuft, kann nicht gewinnen. Ein wirksames Vorgehen, sowohl unter präventiven wie repressiven Gesichtspunkten, fordert fachlich qualifiziertes Personal und eine den Herausforderungen des Kriminalitätsphänomens angemessene technische Ausstattung. Insbesondere im Bereich der Ausbildung bei der Polizei und – diese darf ich miteinbeziehen – bei den Staatsanwaltschaften dürfen wir in unseren Anstrengungen nicht nachlassen. Dies ist angesichts der rasanten technologischen Veränderung und der ständig wechselnden Vorgehensweise der Straftäter keine leichte Aufgabe. Gleichwohl – wir müssen, was das Know-how anbelangt, sozusagen auf Höhe der Zeit und in Augenhöhe sein, um mit Aussicht auf Erfolg antreten zu können. Dazu gehört auch, dass wir mit Nachdruck weiterhin in Forschung und Methodenentwicklung zum rechtzeitigen Erkennen und zur Abwehr neuer Gefahren durch Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnologien investieren. Ich freue mich daher, dass Vertreter aus Wissenschaft und Forschung, mit denen das kriminalistische Institut des Bundeskriminalamtes seit langem Verbindung hält und kooperiert, an unserer Veranstaltung teilnehmen. Seien Sie uns herzlich willkommen.

Die Verfolgung von IuK-Kriminalität, ja schon die Aufdeckung von strafrechtlich relevanten oder die Sicherheit des Staates und der Gesellschaft tangierenden Kommunikationen, etwa mit extremistischem oder terroristischem Hintergrund, stoßen häufig auf Belange des Datenschutzes und – ich will es nicht verschweigen – auf nicht immer deckungsgleiche Interessen der Wirtschaft. Wir wollen uns mit diesen Aspekten im Verlauf der Tagung befassen. Ich darf bei dieser Gelegenheit ganz besonders herzlich den Bundesbeauftragten für den Datenschutz, Herrn Dr. Jakob, begrüßen. Sie werden, verehrter Herr Dr. Jakob, heute das letzte Mal in amtlicher Eigenschaft an einer Tagung des Bundeskriminalamtes teilnehmen. Ich möchte Ihnen für die jahrelange offene und faire, von Verständnis für unsere Belange geprägte Zusammenarbeit danken.

Meine Damen und Herren,

der Rahmen, in den Strafverfolgungs- und Sicherheitsbehörden bei der Bekämpfung der Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnologien gestellt sind, wird durch den Gesetzgeber vorgegeben. Die wie in einem Dreieck stehenden Anliegen des Daten- und Persönlichkeitsschutzes, die Interessen der Wirtschaft und die Belange der Sicherheits- und Strafverfolgungsbehörden fordern immer wieder Abwägungsprozesse, um zu möglichst sachgerechten Lösungen zu kommen. Ein, wie wir wissen, nicht leichtes Unterfangen. Nicht nur die Polizei, sondern auch die Nachrichtendienste, für die ich hier stellvertretend den Präsidenten des Bundesamtes für Verfassungsschutz, Herrn Fromm, begrüße, sind bei diesem Prozess insbesondere mit der Dynamik der Entwicklung im IuK-Bereich und mit einem von großer Flexibilität geprägten

Täterverhalten konfrontiert. Die Sicherheitsbehörden sehen ihre Aufgabe darin, beratend ihre Erfahrungen in den politischen Meinungsbildungsprozess einzubringen, der jeder Rechtsetzung vorausgeht. Allein vor diesem Hintergrund ist unser Tagungsthema auch ein hochpolitisches, weshalb ich mich freue, dass die Politik unserer Einladung gefolgt ist, an der Spitze der Herr Bundesminister des Innern. Herr Minister Schily, ich darf Sie auf das Herzlichste begrüßen. Wir freuen uns, dass Sie gleich zu uns sprechen werden.

Mit gleicher Freude darf ich die Abgeordnete Frau Köhler und die Herren Abgeordneten des Deutschen Bundestages herzlich begrüßen. Meine Damen und Herren, wir betrachten unsere Arbeitstagung als ein Forum des Informations- und Meinungsaustauschs, als eine Möglichkeit, Probleme zu identifizieren und Lösungsvorschläge zu erarbeiten. Ich bedanke mich für die spontane Zusage der Referenten und wünsche uns allen drei interessante informationsreiche Tage hier in Wiesbaden. Als Moderator wird uns der Leiter unseres Kriminalistischen Instituts, Herr Prof. Dr. Stock, durch die Tagung führen. Herr Minister, ich darf Sie jetzt bitten, zu uns zu sprechen.

Eröffnungsansprache

Otto Schily

Bundesinnenminister Schily, hier zwischen Festredner Prof. Dr. Glotz und dem Präsidenten des Bundeskriminalamtes, Dr. Kersten, eröffnete die Tagung

Lieber Herr Dr. Kersten,
lieber Peter Glotz,
Kolleginnen und Kollegen des Deutschen Bundestages,
meine Damen und Herren,

auch ich muss betonen: Sie haben ein sehr aktuelles Thema gewählt. Das ist unbestreitbar und ich will es vielleicht so fassen: Wir haben mit diesem Kriminalitätsbereich sozusagen die Schattenseite einer gewaltigen technischen Revolution in Betracht zu ziehen – einer technischen Revolution, von der ich nicht zögere zu sagen, dass sie mindestens die Dimension der Erfindung der Buchdruckerkunst hat. Auch die Erfindung der Buchdruckerkunst hat dazu geführt, dass sich neue Kriminalitätsformen entwickelt haben. Dass diese Kriminalitätsformen sich eben auch konkretisieren, können wir an Ereignissen der allerletzten Zeit ablesen. Die meisten von Ihnen werden Anfang November dieses Jahres die vom Bundeskriminalamt koordinierten Exekutivmaßnahmen gegen Softwarepiraten verfolgt haben, bei denen fünf Haftbefehle vollstreckt, mehrere Personen vorläufig festgenommen und 46 Objekte im Bundesgebiet durchsucht wurden. Neben umfangreichem Beweismaterial wurde unter anderem eine komplette Fälscherwerkstatt entdeckt. Der bisher seitens der Ermittlungsbehörden errechnete Schaden beträgt

etwa 16 Millionen Euro. Die Beschuldigten stehen in Verdacht, seit mehreren Jahren gewerbsmäßig ge- oder verfälschte Computersoftware verschiedener Hersteller in den Handel gebracht zu haben. Das ist eine sehr triviale aber durchaus bedeutsame Kriminalitätsform, die wir hier aufgedeckt haben.

Noch mehr Aufsehen in der Öffentlichkeit erregte die Operation „Marcy", bei der mit einer weltweit angelegten Aktion im September 2003 insgesamt 38 international agierende Tauschzirkel für Kinderpornographie im Internet gesprengt wurden. Diese Operation ist bislang die bedeutendste Aktion gegen die internationale Kinderpornographie-Szene, bei der Deutschland Ausgangspunkt für die Ermittlungen war. Weltweit sind von den Ermittlungen über 160 Staaten mit rund 26.500 Tatverdächtigen betroffen. Die Zahlen, die ich Ihnen soeben genannt habe, sind ein Hinweis auf die abgrundtiefen Dimensionen einer der abscheulichsten Kriminalitätsformen, bei denen Kindern, unschuldigen schwachen Kindern seelische Schäden zugefügt werden, die sie vermutlich ihr Leben lang begleiten. Die internationale Zusammenarbeit wurde dabei vom Bundeskriminalamt koordiniert. Dort wurden auch rund 3.000 E-Mail-Adressen ermittelt, nach Ländern zugeordnet und bislang 2.535 Einzelvorgänge an 61 Staaten mit der Bitte um Einleitung von Strafverfolgungsmaßnahmen übermittelt. Diese Zahlen machen deutlich, vor welche Herausforderungen Strafverfolgungsbehörden gestellt sind, wenn sie gegen die Verbreitung von Kinderpornographie im Internet vorgehen. Auch an der Stelle geht mein besonderer Dank an die ermittelnden Beamtinnen und Beamten. Jeder kann nachvollziehen, dass solche Ermittlungen auch mit erheblichen psychischen Belastungen verbunden sind, wenn man sieht, welch schreckliche Verbrechen an Kindern begangen werden.

Allein diese Beispiele zeigen die Variationsbreite von Informations- und Kommunikationskriminalität. Gemeint sind damit unterschiedlichste strafbare Sachverhalte, die im Kern eines gemeinsam haben: Die Täter nutzen zur Tatvorbereitung oder -begehung moderne Informations- und Kommunikationsmedien einschließlich Internet oder diese sind selbst das Ziel strafbarer Handlungen. Die neuen Kommunikationsformen machen sich Kriminelle zu Nutze, nicht nur sozusagen zur kriminellen Kommunikation untereinander, sondern auch zum Angriff auf Kommunikationswege und Datenbestände. Die Bandbreite krimineller Machenschaften ist besorgniserregend. Sie reicht von der Verbreitung von Viren über Trojaner bis hin zur unbefugten Veränderung von Webseiten, von illegalen Glücksspielen über Bauanleitungen für Bomben bis hin zur Verbreitung rechtsextremistischen Gedankenguts. Schon diese Beispiele aus zum Teil völlig unterschiedlichen Bereichen zeigen die Spannbreite des Begriffs der IuK-Kriminalität. IuK-Kriminalität beschränkt sich nicht, wie vielfach aufgrund der Medienberichterstattung angenommen, auf Internetkriminalität und auch nicht auf die abscheulichste Form: die Verbreitung von Kinderpornographie.

Der bisherige Anstieg der Fallzahlen zur Computerkriminalität hat sich in der Polizeilichen Kriminalstatistik im Jahr 2002 zwar nicht fortgesetzt. So sind die Fall-

zahlen zur Computerkriminalität insgesamt um über 25 % zurückgegangen. In Teilbereichen sind gleichwohl erhebliche Zuwächse der Fallzahlen zu verzeichnen. Bei den Delikten der Datenveränderung und Computersabotage sind die Fallzahlen gegenüber dem Vorjahr um über 50 %, im Bereich der gewerblichen Softwarepiraterie sogar um 90 % gestiegen. Zudem ist nach wie vor im Bereich der IuK-Kriminalität mit einer erheblichen Dunkelziffer zu rechnen. Die Bedrohung durch IuK-Kriminalität ist daher unverändert groß.

Diese Entwicklung erfordert vor dem Hintergrund bereits bekannt gewordener sowie weiterhin zu erwartender Risiken und Schäden mehr Sicherheit durch verstärkte Repression und Prävention. Fast mehr noch als in der realen Welt spielt für die Akzeptanz der Nutzung dieser meist neuen Technologien das subjektive Sicherheitsgefühl des Einzelnen eine entscheidende Rolle, das neben der objektiven und durch Technik und Regeln bestimmten IT-Sicherheit ausreichend Berücksichtigung finden muss. Das Vertrauen der Nutzer in diese Technologien ist für die weitere Entwicklung der Informationsgesellschaft ein sehr wesentlicher Faktor. Die Strafverfolgungsbehörden müssen durch effektive Bekämpfung von I- und K-Kriminalität dieses Vertrauen fördern.

IuK-Kriminalität zeichnet sich im Gegensatz zu anderen Kriminalitätsformen durch zwei Besonderheiten aus. Zum einen, und dies habe ich bereits erwähnt, ist diese Form der Kriminalität – bedingt durch den schnellen Wandel der IuK-Technologien selbst – einer ständigen und rasanten Entwicklung unterworfen. Eine zweite Besonderheit ist, dass IuK-Kriminalität und hier insbesondere der Bereich der Internetkriminalität in den meisten Fällen ein grenzüberschreitendes Phänomen ist. Ich werde darauf zurückkommen, führt dies doch zwangsläufig zu der Frage, inwieweit nationale Anstrengungen hier erfolgreich sein können. Allzu oft sind Straftäter den Strafverfolgungsbehörden bei der Nutzung neuer Technologien einen Schritt voraus. Die Strafverfolgungsbehörden müssen in die Lage versetzt werden, mit der technischen Entwicklung Schritt halten zu können, sowohl in der Ausstattung als auch in der Ausbildung.

Das kostet Geld – sogar viel Geld, was in Zeiten knapper öffentlicher Haushaltsmittel nicht einfach zu beschaffen ist. Für den Bund kann ich jedoch mit Zufriedenheit feststellen, dass wir in unserem Haushalt für die notwendigen Finanzmittel haben sorgen können, obwohl auch ich auf den ganzen Haushalt bezogen eine Reduzierung von 4 % hinnehmen muss.

Aber nicht nur eine gute personelle und sachliche Ausstattung ist zur effizienten Bekämpfung der IuK-Kriminalität notwendig, sondern auch eine strukturelle Aufstellung, die den Anforderungen genügt. Dazu gehört unter anderem die Einrichtung spezialisierter Dienststellen, die über das erforderliche Know-how verfügen. Hier kann der Bund bereits beachtliche Erfolge vorweisen. Um der Begehung von Straftaten unter Nutzung der IuK-Technologien gezielter begegnen zu können, hat das Bundeskriminalamt die einschlägige personelle und technische Fachkompetenz im „**T**echnischen **S**ervicezentrum **I**nformations- und Kommuni-

kations**t**echnologien“ (kurz: TeSIT) gebündelt. TeSIT leistet vorrangig technische Unterstützung bei Exekutivmaßnahmen und Ermittlungen in Datennetzen. Die Gründung eines solchen Servicezentrums, das kann man jetzt schon sagen, hat sich bewährt. Ein in den Medien bekannt gewordener schauerlicher Fall, bei dem TeSIT entscheidende Ermittlungserfolge erzielen konnte, ist der des „Kannibalen“ aus Rothenburg vom Dezember 2003 des letzten Jahres. Hier waren es Mitarbeiter von TeSIT, die aufgrund eines Hinweises aus der Bevölkerung zu dem zu diesem Zeitpunkt nur unter einer E-Mail-Adresse bekannten Täter Kontakt aufnehmen und seine Identität ermitteln konnten. Ein großer Erfolg! Und ich darf in aller Bescheidenheit darauf hinweisen, dass vielleicht auch einige Länder sich diese Institution zum Vorbild nehmen können. Vielleicht gibt es schon welche, die das getan haben. Diese kleine Empfehlung darf man ja bei der Gelegenheit auch zum Ausdruck bringen.

Zur Aufdeckung von anderen kriminellen Inhalten im Internet hat sich die Innenministerkonferenz 1998 darauf geeinigt, dass das Bundeskriminalamt **z**entrale **a**nlassunabhängige **R**echerchen in **D**atennetzen vornimmt. Anfang 1999 hat die sogenannte ZaRD im Bundeskriminalamt den Wirkbetrieb aufgenommen. Das Bundeskriminalamt wertet das Internet mit derzeit 16 Mitarbeitern rund um die Uhr systematisch und anlassunabhängig auf polizeilich relevante – insbesondere kinderpornografische – Inhalte aus und führt gegebenenfalls die Beweiserhebung, -sicherung und -dokumentation durch. Im Alltagsdeutsch nennt man das „im Internet auf Streife gehen“. Die ZaRD hat in ihrer Arbeit bereits zahlreiche Erfolge vorzuweisen. Bundesweite operative Maßnahmen und Verurteilungen von Herstellern, Verbreitern und Besitzern von Kinderpornographie sprechen für sich. Ich nenne hier nur das Vorgehen gegen den Tausch kinderpornografischen Materials in der Internet-Tauschbörse KaZaa vom April dieses Jahres, in dessen Rahmen bundesweit 57 Tatverdächtige ermittelt werden konnten und gegen die entsprechende Ermittlungsverfahren eingeleitet wurden.

Staatliches Handeln allein kann eine effektive und umfassende Bekämpfung der IuK-Kriminalität allerdings nicht leisten. Es ist daher notwendig, dass staatliche Stellen und Wirtschaftsbeteiligte eng miteinander kooperieren, wie dies auch bereits in einigen Bereichen geschieht. Wirksame Maßnahmen gegen rechtswidrige und jugendgefährdende Inhalte liegen auch im Interesse der Internet-Wirtschaft.

Beispiel einer konstruktiven Zusammenarbeit aller Beteiligten bei der effektiven Bekämpfung der Kriminalität im Internet ist das Projekt „Effiziente Betrugsbekämpfung im Internet“ im Rahmen der Initiative D21. Gemeinsam mit der Firma Ebay erarbeiten unter anderem Fachleute meines Hauses ein Konzept zur Betrugsbekämpfung im Online-Handel mit einem Schwerpunkt auf Aspekten der Prävention.

Die Ansätze sind da. Aber es besteht Bedarf, sie auszubauen und zu erweitern. Lassen Sie mich zwei Punkte herausgreifen:

Punkt eins: Zwar ist nach Auffassung der Bundesregierung die Einführung einer Meldepflicht zur Aufhellung des Dunkelfeldes bei Hackingstraftaten nicht sinnvoll, da die Einhaltung einer solchen Verpflichtung kaum zu kontrollieren wäre. Derartige Kontrollen widersprechen auch der bisherigen Haltung, wonach wir auf dem Gebiet der IT-Sicherheit vertrauensvoll mit der Wirtschaft zusammen arbeiten. Gleichwohl bedarf es ganz allgemein größerer Offenheit seitens der betroffenen Firmen bei der Mitteilung strafbarer Sachverhalte. Zu häufig halten Firmen derartige Erkenntnisse unter Verschluss – mit Rücksicht auf vermeintliche Interessen ihrer Kunden oder aus Angst vor Vertrauensverlusten ihrer Klientel. Nur: staatliche Stellen können repressiv nur einschreiten, wenn ihnen derartige Sachverhalte gemeldet werden. Ansonsten bleiben Aufrüstungsmaßnahmen in diesem Bereich wirkungslos. Die Polizeidienststellen von Bund und Ländern nehmen solche Anzeigen entgegen. Sicherlich müssen diese aber zukünftig noch mehr Professionalität bei der Bearbeitung erwerben.

Punkt zwei: Anbieter von Newsservern durch entsprechende Software sollten automatisiert nach kinder- und tierpornografischen Abbildungen suchen, um Treffermeldungen anschließend an die beim Bundeskriminalamt angesiedelte ZaRD zu übermitteln. Ich appelliere ausdrücklich an das Verantwortungsbewusstsein jedes Wirtschaftsbeteiligten, im Rahmen seines Wirkungskreises einen Beitrag dafür zu leisten, dass strafbare Handlungen im Netz entdeckt und verfolgt werden.

Eine wichtige Rolle für eine effektive Bekämpfung der IuK-Kriminalität im Sinne von Prävention spielt die IT-Sicherheit. Staat und Wirtschaft dürfen nicht warten, bis sich derartige Kriminalität ereignet hat, bis sozusagen das Kind in den Brunnen gefallen ist. Es wäre verfehlt, allein auf Repression zu setzen.

So ist der Schutz der inneren Sicherheit heute untrennbar mit der Förderung und Verbesserung von IT-Sicherheit verbunden. In dem Maße, in dem die Bedeutung von eGovernment und eCommerce zunimmt, steigt auch die Notwendigkeit für eine sichere IT-Infrastruktur. Dabei sind noch viele Aufgaben zu erfüllen. Eine Gesellschaft, die sich in ihrem gesamten technischen, organisatorischen, logistischen Umfeld stark an die Informations- und Kommunikationstechnik bindet, muss an der Stelle auch die Risiken, die damit dann verbunden sind, kompensieren oder mindestens diesen Risiken durch verstärkte Sicherheitsmaßnahmen begegnen.

Bei den beiden großen Angriffen dieses Sommers mit den Viren „Blaster“ und „Lovsan“ waren hauptsächlich Privatanwender betroffen, die – im Gegensatz zu der Mehrzahl der Unternehmen – keine geeigneten Sicherheitsmaßnahmen ergriffen hatten – und das, obwohl die Schwachstelle vorher bekannt war. Das bedeutet: Der sachgerechten Aufklärung und Sensibilisierung vor Gefahren durch staatliche Stellen, aber auch durch die Softwareindustrie selbst muss mehr Bedeutung zukommen als bisher.

Wenn wir die Unternehmen befragen, dann bescheinigt die überwiegende Mehrzahl von ihnen der Informationssicherheit einen hohen Stellenwert. Das ist das erfreuliche Ergebnis einer jüngst veröffentlichten Studie. Doch obwohl fast alle Unternehmen IT-Sicherheit für äußerst wichtig halten, gibt ein Drittel der Befragten in der gleichen Studie zu, auf einen IT-Angriff nur unzureichend reagieren zu können. Ebenfalls ein Drittel der Unternehmen hat nur bedingt einen Überblick darüber, ob die eigenen Systeme gerade attackiert werden oder nicht. Als Hauptgrund für die mangelhafte IT-Sicherheit nennt mehr als die Hälfte der Befragten unzureichende finanzielle Ressourcen.

Solche Versäumnisse in der IT-Sicherheit dürfen wir uns als moderne Wirtschaft, aber auch als staatliche Verwaltung nicht leisten. Das steigende Ausmaß der IT-Attacken zeigt, dass Staat, Wirtschaft und Gesellschaft sich gegen Anschläge auf ihre Datennetze wappnen müssen.

Bei der Frage nach dem Stand der IT-Sicherheit in Deutschland müssen wir aber auch klare Verantwortlichkeiten zuweisen. Es muss klar sein, wer an welcher Stelle für den Schutz von Daten, Informationen und IT-Infrastrukturen verantwortlich ist. Neben den Betreibern der IT-Systeme sind das vor allem die Hersteller und Entwickler von IT-Systemen. Sie müssen bereits bei der Konzeption ihrer Produkte und Systeme Sicherheit als festen Bestandteil begreifen und berücksichtigen. Verantwortlich ist aber auch jeder einzelne Nutzer. Als Teil des weltweiten Informationsnetzes können von jedem Internet-PC Gefahren für die Sicherheit des Netzes in seiner Gesamtheit ausgehen. Die Botschaft lautet: IT-Sicherheit beginnt zu Hause und im Betrieb.

Eine sichere und damit zukunftsgerichtete Informationsgesellschaft in Deutschland liegt in der gemeinsamen Verantwortung von Staat und Verwaltung, Wirtschaft und Industrie, Bürgerinnen und Bürgern.

Für die Bundesregierung kann ich sagen: Wir sind gut aufgestellt. Nach den Ereignissen des 11. September 2001 haben wir die Maßnahmen und Programme zur Förderung der IT-Sicherheit noch einmal deutlich erhöht. Im Bereich der Bundesverwaltung haben wir das Bundesamt für Sicherheit in der Informationstechnik personell und sachlich ausgebaut. Im Rahmen der Antiterrormaßnahmen haben wir die Mittel des BSI im Jahr 2002 um fast 40 % erhöht. Das BSI hat sich als zentraler IT-Sicherheitsdienstleister der Bundesregierung etabliert. Mit seiner umfassenden Kompetenz für alle Fragen der IT-Sicherheit ist das BSI einzigartig in Europa. Das BSI leistet einen Beitrag auf „breiter Front“, um die IT-Sicherheit in Deutschland effektiv zu verbessern. Es ist überdies Vorbild für die demnächst zu gründende europäische IT-Sicherheitsagentur ENISA – die Europäische Agentur für Netz- und Informationssicherheit. Und ich bin froh darüber, dass damit eine Initiative, die von Deutschland ausgegangen ist, auf europäischer Ebene verwirklicht wird, wie viele andere übrigens auch.

Eine enge Kooperation mit der Wirtschaft haben wir in den vergangenen Monaten beim Schutz kritischer Infrastrukturen erzielt. Das ist ein Bereich, in dem die Aspekte „Sicherheitsbedürfnis“ und „Schutz der Gesellschaft“ sehr deutlich in den Vordergrund zu rücken sind. Kritische Infrastrukturen sind im besonderen Maße auf sichere und vor allem ausfallsichere IT-Informationstechnik angewiesen. In Deutschland befinden sich 80 Prozent der kritischen Infrastrukturen in privatwirtschaftlicher Hand. Unmittelbar im Anschluss an die terroristischen Angriffe im Jahr 2001 habe ich mit den Betreibern der wichtigsten Infrastrukturen unseres Landes Fragen eines verlässlichen Schutzes aller Infrastrukturbereiche erörtert. Der Bund hat hierbei wegen der gesamtstaatlichen Bedeutung lebenswichtiger Infrastrukturen eine besondere Rolle. Daher wird der Schutz kritischer Infrastrukturen ein Schwerpunkt des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe – kurz BBK – sein. Zusätzlich habe ich das BSI beauftragt, die IT-Abhängigkeit kritischer Infrastrukturbereiche in gesonderten Studien zu untersuchen. Die Ergebnisse dieser insgesamt sieben KRITIS-IT-Studien haben wir im Juli dieses Jahres den Wirtschaftverbänden vorgestellt und eine enge Kooperation auch zu diesem Aspekt vereinbart.

Wir werden noch einen Schritt weiter gehen. Die bisherigen Maßnahmen und die vereinbarten Kooperationsprojekte mit der Wirtschaft werden wir in einem nationalen KRITIS-Plan zusammenfassen. Er wird Richtlinie sein für die Gewährleistung von Sicherheit und Verlässlichkeit lebenswichtiger IT-Infrastrukturen.

Ein weiteres erfolgreiches Beispiel für die gute Zusammenarbeit zwischen Staat und Wirtschaft auf dem Gebiet der IT-Sicherheit ist der im Sommer 2002 gegründete CERT-Verbund, der mittlerweile auf zehn Mitglieder angewachsen ist. Den Computer Emergency Response Teams aus Forschung, Wissenschaft und Industrie sowie unserem CERT-Bund ist es in den vergangenen zwölf Monaten gelungen, einen intensiven Informationsaustausch aufzubauen. In Kürze nimmt zudem das Mcert – das CERT für alle mittelständischen Unternehmen in Deutschland – seinen Betrieb auf. Die Ergebnisse zahlreicher Umfragen zeigen immer wieder, dass viele deutsche Unternehmen Nachholbedarf haben bei der Sicherheit ihrer IT-Systeme. Werkzeuge und Hilfsmittel stehen zur Verfügung – nicht zuletzt durch die Arbeit des BSI.

Im Gegensatz zur Wirtschaft gibt es bei privaten Nutzern in der Regel keine professionelle Betreuung der Informationstechnik. Entsprechend groß ist hier der Bedarf an fachgerechter Beratung und Aufklärung. Gerade im privaten Bereich hat ein Großteil der IT-Anwender nur rudimentäre Kenntnisse über die im Internet drohenden Gefahren und über angemessene Schutzmaßnahmen. Für diese Zielgruppe hat das BSI eine Sicherheits-CD entwickelt, mit der insbesondere Internet-unerfahrene Bürgerinnen und Bürger für das Thema „IT-Sicherheit“ sensibilisiert werden sollen und von der bis heute bereits 1,22 Millionen verteilt wurden – eine beachtliche Zahl. Und ich hoffe, dass sie eben nicht nur entgegengenommen

werden, sondern dass sich die Menschen auch anhand dieser Sicherheits-CD entsprechend einstellen können und werden.

Meine Damen und Herren, Prävention und Repression sind zwei Seiten ein und derselben Medaille. Um optimale Ergebnisse bei der Bekämpfung der Hochtechnologie-Kriminalität zu erzielen, brauchen wir beide. Auch die beste Prävention macht eine wirkungsvolle Verfolgung von Straftaten, die trotz ausgeklügelter Schutzvorkehrungen begangen werden, nicht entbehrlich. Ich trete deshalb dafür ein, Instrumente an die Hand zu geben, die nötig sind.

Wir müssen Telekommunikationsüberwachungsmaßnahmen erlauben bei Verdacht bestimmter Straftatbestände, die entweder typischerweise unter Benutzung von Informations- und Kommunikationsmedien vorbereitet bzw. begangen werden oder bei denen diese Medien selbst das Angriffsziel der Straftat sind. Ich denke hierbei an die Verbreitung kinderpornografischer Schriften sowie an Computersabotage, das Ausspähen von Daten und Datenveränderung. Die anstehende Revision der Vorschriften der Strafprozessordnung zur Telekommunikationsüberwachung, die die Konsequenzen aus den Erkenntnissen des Gutachtens des Max Planck-Instituts vom Mai dieses Jahres ziehen wird, erscheint mir hierfür eine gute Gelegenheit.

Auch der Regierungsentwurf für das Telekommunikationsgesetz sieht für eine effektive Strafverfolgung von IuK-Kriminalität wichtige Vorschriften über die Auskunftsrechte der Strafverfolgungsbehörden vor. Wir brauchen im Rahmen der automatisierten Abfrage bestimmter personenbezogener Daten die Möglichkeit, Abfragen der Strafverfolgungs- und Sicherheitsbehörden mit Hilfe unvollständiger und ähnlicher Abfragedaten durchzuführen. Auch müssen wir geschäftsmäßige Anbieter von Telekommunikationsdienstleistungen für die Öffentlichkeit dazu verpflichten, bestimmte für die Strafverfolgung wichtige Kunden-Daten zu erheben und speichern, unabhängig davon, ob diese Daten für Abrechnungszwecke benötigt werden. Welches Ausmaß das haben kann und soll, darüber wird allerdings noch zu sprechen sein.

Unakzeptabel für die Strafverfolgungsbehörden ist, dass für eine effektive Bekämpfung der IuK-Kriminalität wichtige Verbindungsdaten aufgrund datenschutzrechtlicher Bestimmungen oftmals bereits gelöscht worden sind, wenn sie von den Strafverfolgungsbehörden angefordert werden. In der Praxis nehmen die Strafverfolgungsbehörden in solchen Fällen bisweilen direkten Kontakt zu dem Provider auf und bitten, von einer Löschung dieser Daten bis zu einem Auskunftsersuchen abzusehen. Dieses bislang in der Praxis vorgenommene „Einfrieren der Verbindungsdaten“ ist unverzichtbar. Wir brauchen daher eine klare gesetzliche Grundlage, ähnlich wie sie bereits auf dem Gebiet der Wertpapieraufsicht besteht.

Die weitergehende Frage, ob darüber hinaus Mindestspeicherungsfristen für Verbindungsdaten zu schaffen sind, ist noch nicht abschließend entschieden. Für eine

effektive Strafverfolgung im Internet ist eine solche Mindestspeicherungsfrist aus polizeilicher Sicht von erheblichem Vorteil, in bestimmten Fällen sogar notwendig, da ansonsten keine weiteren Ermittlungsansätze vorhanden sind. Hier ist eine ganze Reihe bedeutsamer Rechtsgüter und tatsächlicher Gegebenheiten abzuwägen.

Immer wieder gefordert wird von Seiten der Strafverfolgungsbehörden eine Zulassungspflicht für Verschlüsselungsprodukte bei gleichzeitiger Verpflichtung zur Hinterlegung des Schlüssels. Dies ist jedoch kein Bereich, in dem eine verschärfte gesetzliche Regelung eine Lösung ist. Eine solche Zulassungs- und Schlüsselhinterlegungspflicht zur Sicherstellung des staatlichen Zugriffs auf verschlüsselte Daten kann der Strafverfolgung nicht weiterhelfen. Verbunden mit einem vielleicht sogar strafbewehrten Verbot der Nutzung nicht zugelassener Produkte mag dies zwar auf den ersten Blick verlockend erscheinen. Doch dieser schon seit vielen Jahren diskutierte und national wie international auch bereits mehrfach verworfene Ansatz berücksichtigt die technischen Realitäten nicht. Die weite Verbreitung von Verschlüsselungsmöglichkeiten, die von derartigen Regelungen nicht erfasst würden, macht eine Umgehung viel zu leicht, als dass sich hier effektive Regelungen aufstellen ließen. Und an unwirksamen Gesetzen können wir alle kein Interesse haben.

Hier brauchen wir andere, praktikable Lösungen. Einerseits müssen wir die Strafverfolgungsbehörden in die Lage versetzen, kryptierte Telekommunikation als solche zu erkennen. Andererseits muss das BSI gemeinsam mit den Strafverfolgungsbehörden effektive Tools entwickeln und bereitstellen, die eine Entschlüsselung dieser Kommunikation ermöglichen.

Eine für die Praxis wichtige Änderung wird im Hinblick auf den Computerbetrug erfolgen. Das Bundeskabinett hat beschlossen, das Herstellen, Verschaffen, Verwahren und Überlassen von Computerprogrammen, um einen Computerbetrug zu begehen, unter Strafe zu stellen. Damit wird eine Strafbarkeitslücke geschlossen. Das Bundeskriminalamt hat zudem im Rahmen des Antiterrorgesetzes die originäre Ermittlungsbefugnis in bestimmten Fällen der Computersabotage erhalten, die für unser Gemeinwesen eine besondere Bedrohung darstellen. Auch in Zukunft werden wir die notwendigen rechtlichen, aber auch organisatorischen und finanziellen Maßnahmen ergreifen, um der IuK-Kriminalität effektiv entgegenzutreten.

Gesetzgeberische Maßnahmen allein auf nationaler Ebene werden dem Problem IuK-Kriminalität aber nicht gerecht, denn IuK-Kriminalität und hier insbesondere Internetkriminalität ist überwiegend eine internationale Erscheinung. Unsere nationalen Gesetze zur Bekämpfung der Internetkriminalität enden an unseren territorialen Grenzen. Die weltweiten Datenverbindungen hingegen überspringen diese mit Leichtigkeit. Das Internet umspannt unseren Globus inzwischen wie ein Spinnennetz. Infolgedessen machen auch die Internet-Kriminellen nicht Halt vor unseren nationalen Grenzen. Eine örtliche Nähe des Täters zu sei-

ner Tat ist bei diesen Straftaten nicht mehr zwingend. So wie internationale Unternehmen weltweit gültige Sicherheitsstandards entwickeln, müssen wir bei der Kriminalitätsbekämpfung und der Schaffung der dazu notwendigen Gesetze der Globalisierung Rechnung tragen.

Die verschiedenen nationalen Gesetze weisen beträchtliche Unterschiede auf. Dadurch werden effizientere Ermittlungen gefährdet. Wir brauchen deshalb eine Harmonisierung des materiellen Strafrechts in diesem Bereich sowie entsprechende strafprozessuale Vorschriften. In Europa können wir damit vorangehen. Die Rechtshilfe muss für Fälle der Computerkriminalität beschleunigt werden. Internationale Verträge in diesem Bereich müssen von möglichst vielen Staaten ratifiziert werden, damit die Entstehung von „sicheren Häfen" für Hochtechnologie-Kriminelle vermieden wird.

Die Arbeit der Organisationen auf internationaler Ebene wie Europarat und G 8 im Kampf gegen Computerkriminalität ist daher zu forcieren. Einen Meilenstein stellt hier insbesondere die Konvention zur Bekämpfung der Datennetzkriminalität des Europarats als erster globaler Ansatz dar, das Spannungsverhältnis von grenzüberschreitenden Computerstraftaten einerseits und Territorialitätsprinzip andererseits zu überwinden. Das Übereinkommen schafft gemeinsame strafrechtliche Mindeststandards zwischen den Mitgliedstaaten des Europarates und den weiteren Vertragsstaaten im Bereich des Computer- bzw. Telekommunikationsstrafrechts. Darüber hinaus entwickelt es gemeinsame Grundlagen für rasche und effektive strafrechtliche Ermittlungen in Computersystemen. Auf dieser Basis wird die internationale Zusammenarbeit in einschlägigen Strafsachen, insbesondere auch mit den Vertragsstaaten, die nicht dem Europarat angehören, wie etwa den Vereinigten Staaten, verbessert. Für die Polizei sehr wichtig ist die Aufnahme verfahrensrechtlicher Regelungen in das Übereinkommen: Für eine beschleunigte und effektive Aufklärung von Computerstraftaten, allerdings nicht nur von diesen, ist ein schneller Zugriff auf Computerdaten in Computersystemen oder Datenträgern zwingend erforderlich. Strafprozessuale Eingriffsbefugnisse in vielen Staaten gestatten derzeit noch nicht die unverzügliche Sicherstellung und Beschlagnahme dieses Datenmaterials. Der verfahrensrechtliche Teil der Konvention enthält daher Regelungen über die Durchsuchung von Computersystemen einschließlich on-line-Durchsuchungen und die Beschlagnahme sowie die Anordnung der Herausgabe von gespeicherten Daten und deren vorläufige Sicherstellung, insbesondere auch von Verbindungsdaten.

Deutschland hat die Konvention bereits unterzeichnet. Die Bundesregierung will das Übereinkommen noch in dieser Legislaturperiode in nationales Recht umzusetzen. Dies bedingt auch Änderungen des deutschen Rechts. Zu nennen sind insbesondere Ergänzungen des geltenden Computerstrafrechts im Hinblick auf Regelungen über den unerlaubten Zugang zu Computersystemen, das unbefugte Erfassen und Aufzeichnen von Datenübertragungen, die Computersabotage sowie die Aufnahme bestimmter Vorbereitungshandlungen. Wo nötig, müssen wir das

Prozessrecht anpassen, nicht zuletzt, um auch eine Beschleunigung der internationalen Zusammenarbeit zu garantieren.

Mit Rücksicht auf die Vereinigten Staaten, die die sog. Cybercrime Konvention des Europarates ebenfalls unterzeichnet haben, und ein dort durch die Verfassung geschütztes, für unsere Maßstäbe sehr weit reichendes Recht auf freie Meinungsäußerung, das uns ja manchmal in der Bekämpfung von Rechtsextremismus ein Problem bereitet, wurden Maßnahmen gegen den Missbrauch von Datennetzen zur Verbreitung rassistischer und fremdenfeindlicher Inhalte zunächst nicht in die Konvention aufgenommen. Der Europarat hat daher, nicht zuletzt aufgrund des Betreibens von Deutschland, ein entsprechendes Zusatzprotokoll erarbeitet. Dieses ist von Deutschland ebenfalls bereits gezeichnet worden.

Ziel des Zusatzprotokolls gegen Rassismus ist es, speziell die Verbreitung rassistischer Propaganda zu verhindern, die missbräuchliche Speicherung von Hassbotschaften zu verbieten und die Benutzung des Internets zur Förderung des Rassismus unter Verbot zu stellen. Gefordert ist ein Vorgehen gegen illegales Hosting, damit Rechtsextremen die Möglichkeit genommen wird, mit ihren Webseiten in ein anderes Land mit weniger strengen Gesetzen auszuweichen. Ich bin der Auffassung, dass dieses Zusatzprotokoll, mit dem das Strafrecht auch auf diesem Gebiet ein Stück weit harmonisiert wird, eine wichtige Ergänzung der Konvention des Europarates darstellt.

Neben dem Europarat ist insbesondere die G 8 - Kooperation für die Bekämpfung der IuK-Kriminalität von Bedeutung. Lassen Sie mich zwei konkrete Vorhaben aus diesem Bereich nennen:

Die Schnelligkeit und Vergänglichkeit elektronischer Beweismittel erfordern Echtzeit-Hilfe durch ein globales Netzwerk und den Einsatz von Kontaktstellen, die sich rund um die Uhr untereinander über Sachverhalte mit Bezug zur Computerkriminalität austauschen. Aus diesem Grund haben die G 8 - Staaten eine entsprechende Struktur ins Leben gerufen und sie darüber hinaus auf eine ganze Reihe weiterer Länder ausgedehnt. Sie umfasst derzeit 35 Staaten. Ziel ist die rasche Erkennung von Fällen der Computerkriminalität, um Strafverfolgungsmaßnahmen rasch einzuleiten. Stetiger Ausbau und Fortentwicklung des Kontaktnetzes ist ein wichtiges deutsches Anliegen.

Auf der Ebene der G-8 habe ich – zusammen mit meinem italienischen Innenministerkollegen – die Errichtung einer internationalen Datenbank zur Bekämpfung der Kinderpornografie auf den Weg gebracht. Diese Initiative ist wesentlicher Teil der Umsetzung der G 8 - Strategie zur Bekämpfung des Missbrauchs von Kindern im Internet. Die Datenbank soll Bilder von missbrauchten Kindern, Tätern und Tatorten sammeln und unter anderem nach biometrischen Merkmalen erfassen. Die Arbeiten, die auf eine Anbindung der Datenbank an Interpol abzielen, sind auf einem guten Weg. Deutschland wird sich hieran auch weiterhin aktiv beteiligen.

Auch innerhalb der EU sind wir aktiv. Die EU fördert die neuen Informationstechnologien für die Entwicklung ihrer Beziehungen mit der Welt und zur Stärkung der Vorteile der freien Verbreitung von Informationen ohne Beeinträchtigung der Sicherheit. Es wurden allerdings zunächst nur rechtsetzende Maßnahmen mit mittelbaren Auswirkungen auf die Computerkriminalität ergriffen. Mit der beschlossenen Verlängerung des Aktionsplans zur sicheren Nutzung des Internet werden unter anderem Projekte zur Entwicklung und vergleichenden Bewertung von Filtersystemen, ein europäisches Meldestellennetz für illegale Inhalte und Strukturen der Selbstkontrolle der Internet-Provider gefördert. Während sich das Vorläuferprogramm schwerpunktmäßig mit dem Jugendschutz und der Bekämpfung von Kinderpornografie befasste, werden nunmehr auch andere illegale und schädliche Inhalte, etwa rassistische oder gewaltverherrlichende Webseiten, thematisiert.

Die Europäische Union muss bei der Bekämpfung der Computerkriminalität noch deutlicher Profil gewinnen. Ein wichtiger Schritt hierzu ist der Vorschlag der Kommission für einen „Rahmenbeschluss des Rates über Angriffe auf Informationssysteme“, der in Kürze verabschiedet werden soll. Ziel ist die Angleichung der Strafrechtsvorschriften in der Europäischen Union und die Unterstützung der Strafverfolgungs- und Justizbehörden im Hinblick auf den unbefugten Zugang zu Informationssystemen, die unbefugte Behinderung oder Störung des Betriebs von Informationssystemen und die unbefugte Datenmanipulation.

Eine herausgehobene, weiter entwicklungsfähige Rolle bei der Bekämpfung der Computerkriminalität spielt auch Europol. Europol hat unter anderem die Zuständigkeit, die Ermittlungen der Strafverfolgungsbehörden der Mitgliedstaaten im Bereich des Menschenhandels zu unterstützen, insbesondere auch in Fällen der Ausübung von sexueller Gewalt gegen Minderjährige. Europol kann bei der Bekämpfung der Kinderpornografie, die das Internet als Kommunikationsmedium nutzt, bereits Erfolge vorweisen: So wurden im Jahr 2002 bei der Operation „Twins“, bei der Europol den Informationsfluss der beteiligten vierzehn Staaten koordinierte, allein in Deutschland 31 Tatverdächtige verhaftet. Europol führt im Bereich der Bekämpfung von Kinderpornografie regelmäßig Fortbildungsseminare für Polizeibeamte der Mitgliedstaaten und der Beitrittskandidaten durch. Durch Erweiterung der Zuständigkeiten von Europol durch Ratsbeschluss vom 6. Dezember 2001 ist Europol nun auch für Computerkriminalität im engeren Sinne zuständig.

Meine Damen und Herren,

ein Zaubermittel zur Bekämpfung und Vermeidung von IuK-Kriminalität gibt es nicht. Wir müssen vielmehr an einer Vielzahl verschiedener, einzelner Punkte die Hebel ansetzen. Dabei geht es keineswegs nur um Rechtsänderungen. Mindestens ebenso wichtig sind praktische Maßnahmen. Eines jedenfalls steht fest: Die Dynamik der IuK-Technologien und ihre Internationalität stellen uns vor nie gekannte Herausforderungen. Sie zu erkennen, in ihrer Tragweite richtig ein-

zuschätzen und die angemessenen Maßnahmen zu ergreifen, ist mit Aufgabe der diesjährigen BKA-Herbsttagung, für die ich einen fruchtbaren Konferenzverlauf wünsche. Wie überall, liegen bei einer neuen Technik Chancen und Risiken nahe beieinander. Das ist kein Grund, auf die Chancen einer neuen Technik zu verzichten, sondern es kommt darauf an, die Chancen zu maximieren und die Risiken zu minimieren.

Vielen Dank!

Festvortrag

Schöne neue Welt? Visionen einer vernetzten Zukunft

Peter Glotz

Herr Präsident, Herr Bundesminister, meine Damen und Herren. Ich bedanke mich herzlich für diese Einladung zum BKA. Herr Minister Schily und ich haben vorhin eine kleine philosophische Betrachtung untereinander angestellt. Wir haben uns vor Jahrzehnten beim Goethe-Institut kennen gelernt. Jetzt treffen wir uns im Herbst unseres Lebens im BKA. Den Zusammenhang mag Otto Schilys Satz stiften: „Wer Musikschulen schließt, gefährdet die Innere Sicherheit."

Wenn ich jetzt über Informations- und Kommunikationstechnik spreche, kann kein Zweifel darüber bestehen, dass diese Informations- und Kommunikationstechnik unsere Gesellschaft insgesamt tief gehend verändert und verändern wird. Das ist die prägende Technologie dieser Jahre. Minister Schily hat von Gutenberg gesprochen. Man könnte auch von der Uhr oder von der Dampfmaschine sprechen. Erst als Uhren auf Kirchtürmen angebracht waren, entstand so etwas wie eine rational geordnete Arbeitszeit. Und die veränderte den Alltag der Menschen! Und ganz ähnlich ist es in der Tat mit dieser Fülle von Instrumenten, die wir als digitale Technologie bezeichnen (obwohl die Digitalisierung ja nur eine technische Entwicklung ist), und von denen die wichtigsten ohne Zweifel der Computer und die Weiterentwicklung der Telekommunikation von GPRS zu UMTS usw. ist. Das heißt, ich glaube, unsere Gesellschaft muss angesichts dieser Instrumente eine neue Kommunikationskultur entwickeln. Das ist eine andere als die der Industriegesellschaft, weil die entscheidenden Aktivitäten von uns allen sich ändern werden. Das geht von Arbeiten, Spielen, Sich-Unterhalten, Lernen, Kommunizieren bis zum Politisieren – und selbstverständlich wäre die Behauptung, dass die Entwicklung zur vernetzten Zukunft konfliktlos verliefe oder dass sie den Menschen nur Vorteile brächte, haltlos. Immer – auch das hat Otto Schily gesagt – geht es um Emanzipations- und Destruktionspotenziale. Aber – und das ist meine Eingangsthese, meine Damen und Herren – wer sie wie unsere Utopisten von Campanella bis zu Aldous Huxley, von dem ja der Begriff „Schöne neue Welt" stammt, – wer das alles vor allem als Apokalypse interpretiert, der produziert eingängige, aber fragwürdige Welterklärungen. Sie können wunderbare Filmdrehbücher für Steven Spielberg schreiben über den Cyber War. Die Wirklichkeit werden Sie damit nicht treffen, wenn auch vielleicht die Gefühle der Menschen. Und deswegen will ich am Anfang einfach zwei persönliche Erfahrungen schildern.

Das eine ist: Ich war im Bundestag eine Zeit lang im Auswärtigen Ausschuss für den Balkan zuständig. Da stellten wir fest, wie sich die Studenten in Belgrad mithilfe ihrer PCs gegen Milosevic, gegen die Diktatur gewehrt haben, wie sie ihre Demonstrationen organisierten, wie sie international verflochten mit der Wharton School in Philadelphia blitzschnell die Informationen aus Belgrad in die ganze

Welt brachten. Das ist Befreiungspotenzial. Das heißt, meine These ist – nehmen Sie jetzt mal nicht Huxley, nehmen Sie Orwell – die Idee vom großen Bruder funktioniert nicht. Ich behaupte, kein Propagandaminister wird jemals wieder so viel Macht haben wie Josef Goebbels in Deutschland, weil diese Abschottungsmöglichkeiten, die gegeben waren, indem man („Feind hört mit") das Abhören von Fremdsendern verbot und die Leute ins KZ schickte, indem man die ganze Presse und den ganzen Rundfunk in der Hand hatte, nicht mehr gegeben sind. Dies wird auch in autoritären Regimen, die es heute noch – nicht nur dutzendweise, sondern hundertweise – in der Welt gibt, nicht mehr möglich sein. Das ist ein Hinweis darauf, dass die negative Utopie nicht eintreten muss. Ein zweites Beispiel zeigt aber auch das, was Sie Herr Präsident gezeigt haben: das Dreieck. Also die Zivilgesellschaft mit ihren Grundrechten und persönlichen Interessen, die Wirtschaft und dann die Sicherheitsinteressen, die ja auch Interessen der Bevölkerung sind; aber oft wird das ja gegeneinander gespielt. Ich habe gerade eine große Untersuchung gemacht über Webauftritte von Zeitungen. Und Sie wissen, unsere Zeitungen sind in einer schweren Krise, weil die Anzeigen wegbleiben, weil künftig die Rubrikenanzeigen gänzlich aufs Internet gehen werden. Meine Damen und Herren, wie die New York Times die Adressen derer, die ihre Website anklicken und deren Konsumgewohnheiten systematisch nutzt: Das kann sich eine deutsche Zeitung überhaupt nicht vorstellen. Stichwort Datenschutz. Das, was die dürfen, darf man bei uns nicht. Das sind die Interessen der Wirtschaft.

Prof. Dr. Peter Glotz von der Universität St. Gallen hielt den Festvortrag

Sie haben gefragt, Herr Präsident: Wie geht das weiter? Es gibt mehrere Delphi-Umfragen dazu, das heißt Umfragen bei den wirklichen Experten, die an diesen

Schnittstellen arbeiten. Wir werden in diese digitale Gesellschaft erst eintreten mit Wirksamkeit für die ganze Gesellschaft, also für die große Mehrheit der Gesellschaft, in den Jahren 2009 bis 2014. Das betrifft jetzt die Diffusion der schon längst bekannten Techniken in die Gesellschaft hinein. Noch immer sind wir bei vielen dieser Techniken bei den Early adapters. Noch immer gibt es viele Menschen älterer Jahrgänge, aber auch unterschiedlicher sozialer Schichten, die diese digitale Technologie noch nicht oder kaum nutzen. Zudem sage ich, dass wir beim Electronic Government noch bei den ersten Schritten sind. Wir haben wunderbare Modellgemeinden. Wir sind auch weiter als manch andere Länder. Aber natürlich, vieles muss erst noch kommen. Ich habe mir gerade – ich lebe ja in der Schweiz – den Pass an dem letzten Ort erneuern lassen, an dem ich gewohnt habe: in München. Da müssen Sie immer noch mit dem Auto zum Kreisverwaltungsreferat herunterfahren, müssen dort einen Parkplatz suchen, reingehen, eine Nummer ziehen. Dann kommen Sie nach anderthalb Stunden dran. Dann müssen Sie ein Formular abgeben mit zwei Fotos, Passbildern. Und nach 14 Tagen müssen Sie das noch mal machen. Electronic Government? Das ist keine Kritik an den Institutionen. Ich weiß genau, woran es hapert. Ich weiß genau, wie schwierig es ist, die Investitionen aufzubringen, in welche Diskussionen man mit den Gewerkschaften gerät usw. Ich will nur sagen: Das verstärkt eigentlich die Notwendigkeit der Diskussion, die Sie führen wollen, Herr Präsident. Die Diffusion der modernen Apparate in die Gesellschaft hinein, wird erst am Ende dieses Jahrzehnts bei uns stattfinden, in den Vereinigten Staaten und vielleicht auch in dem einen oder anderen skandinavischen Land noch ein bisschen früher. Aber wir sind noch nicht ganz drin.

Jetzt im Dezember findet diese berühmte Konferenz WSIS (World Summit of Information Society) statt. Die wird nur zeigen, wo die Problemlage ist und das Dreieck Ihres Präsidenten. Dort nämlich gibt es eine wichtige und heftige Auseinandersetzung zwischen den Entwicklungsländern auf der einen Seite, die von den großen Gesellschaften verlangen, einen Solidaritätsfonds aufzustellen, um den „Digital Divide“ zu überbrücken. Das werden die großen Länder nicht wollen. Die zweite Auseinandersetzung – und das ist die entscheidende – ist die klassische. Dass nämlich die Staaten mit autoritären Systemen, die nicht Demokratie verwirklicht haben wie viele europäische Staaten oder die Vereinigten Staaten, diese Chance des internationalen Austausches, die gegeben ist dadurch, dass Sie jetzt mit dem Fingertipp von München nach Los Angeles über Ihren Computer kommen, dass Sie eine Mail an 1.000 Leute verteilen können, nicht nutzen. Da geht es um die Weltinformationsordnung, über die wir in den Vereinten Nationen schon seit Jahrzehnten diskutieren. Und natürlich wird das dritte Thema dann die Frage des Datenschutzes und des Schutzes der Bürgerrechte sein.

Also, wir sind am Anfang einer wichtigen Entwicklung. Und lassen Sie sich nicht verführen von denen, die euphorisch durch die Gegend liefen zwischen 1995 und 2000. Dann kam der Bubble und es platzte die Blase an den Aktienmärkten. Und dann sagten die plötzlich: Das war alles nur Hysterie. Alles nur Hype, heißt das

heutzutage. Davon kann keine Rede sein. Es war manches Hype, aber wir gehen in eine neue gesellschaftliche Struktur. Die will ich jetzt in ein paar Sätzen zu schildern versuchen.

Meine vier Begriffe, die diese neue Gesellschaft charakterisieren, meine Damen und Herren, heißen: Dematerialisierung, Beschleunigung, Dezentralisierung und Globalisierung. Natürlich, diese Grundtendenzen ergreifen niemals die ganze Gesellschaft. Wir haben heute noch einen kleinen Agrarsektor. Und wir haben einen viel größeren Industriesektor – Gott sei Dank – als manche, die von digitaler Gesellschaft reden, zugeben. Der weltweite Umsatz der Informationsgesellschaft steigt. Der Umsatz der klassischen Industriegesellschaft sinkt. Informationstechnische Industrie ist seit einem Jahrzehnt die größte Industriebranche der Welt. Und sie bestimmt ein immer größeres Segment unserer Gesellschaft. Dematerialisierung heißt, dass ein großer Teil der wirtschaftlichen Tätigkeiten in dieser digitalen Ökonomie nicht mehr von der Verwertung von Bodenschätzen, von Stoffumwandlung bestimmt wird, sondern von der Verwertung von Informationen. Die hardwareorientierte Industriegesellschaft wandelt sich zu einer softwareorientierten Informationsgesellschaft. Das hängt natürlich mit der Miniaturisierung der Mikroelektronik zusammen. Wertschöpfung wird mit einem viel geringeren Energieeinsatz möglich als in der alten Industriegesellschaft. Das war Nummer 1. Jetzt komme ich zu Nummer 2: Beschleunigung. Schauen Sie sich diesen 24-Stunden-Geldmarkt an. Das ist etwas, was wir uns vor zwanzig Jahren nicht vorstellen konnten. Wenn die eine Börse zumacht, macht die andere Börse auf. Die Dominanz der Finanzwirtschaft über die reale Wirtschaft wird immer größer. Das hat natürlich auch dann die entsprechenden Folgen für die Möglichkeiten der Wirtschaftskriminalität. Dies war ohne diese Kommunikationsrevolution nicht möglich. Und dieser Geschwindigkeitsimpuls wirkt sich auf jeden von uns aus. Die Tatsache, dass wir, wenn wir reisten vor zwei Jahrzehnten, unser Büro zwar gelegentlich anrufen konnten über eine Telefonzelle. Das Mobilfunkgerät verwandelt das Leben jedes Menschen und, unter uns gesagt, das Leben des Geringverdieners am Bankschalter, der auch umgehen muss mit Informationstechnik, noch viel mehr als das Leben der Chefs, die sich manches doch noch ersparen können – unter anderem auch den Computer. Ich diktiere meine E-Mails, meine Damen und Herren. Das geht viel schneller, als wenn ich die alle tippen würde. Ich kenne viele Vorstandsvorsitzende und höchstens zwei darunter, die Informationstechnik selber bedienen, obwohl sie alle natürlich einen Computer auf dem Tisch stehen haben. Der steht da für Journalisten. Das heißt in der Tat, es dauert noch einen Moment, bis sich das wirklich verändert hat, denn wenn der/die jetzigen Assistent(en) Vorstandsvorsitzende sind, wird das schon anders sein.

Meine Damen und Herren, es geht um die Beschleunigung des Lebens von uns allen. Die Stichworte heißen Timebased Management, Simultaneous Engineering, Verkürzung der Entwicklungszeiten, Verkürzung der Marktpräsenzseiten. Das verändert unser Leben. Das Leben dieser Menschen, der Wissensarbeiter – und ich vermute, dass das alles Wissensarbeiter sind, die in diesem Saal

sitzen – muss mobil und flexibel sein. Sie dürfen sich nicht beschweren, wenn sie alle fünf Jahre umziehen müssen oder wenn der Hauptverdiener oder die Hauptverdienerin an einem anderen Ort arbeiten als die Familie lebt. Weiterbildung, all das, sind grundlegende gesellschaftliche Veränderungen. Sie werden gleich sehen, warum ich das erzähle. Das ist nämlich auch sicherheitsrelevant. Dezentralisierung sieht anders aus. Die großen Konzerne häufeln sich Schritt für Schritt auf. Sie betreiben Outsourcing, sie geben Gewinn-und-Verlust-Verantwortung in Product divisions, schließlich Globalisierung. Ich sage nur: Lassen Sie uns den Begriff nicht nur ökonomisch, sondern lassen Sie ihn uns kommunikativ fassen. Die bis zum Überdruss zitierten Softwareprogrammierer aus Bangalore, die für ein Minimum der Entlohnung für Siemens arbeiten und für viele andere europäische Konzerne, die gibt es in der Tat. Die Individualisierung wächst. Und plötzlich besteht so eine Gesellschaft nicht mehr aus drei oder fünf Gesellschaften, die man früher Schichten nannte, sondern aus 15 oder 20, die man jetzt Milieus nennt. Das alles hat zu tun mit dieser komischen Technik.

Meine Damen und Herren, ich schließe jetzt diese allgemeine Analyse, indem ich eins sage. Dies alles hat – auch wenn es gelegentlich nicht leicht ist, es zuzugeben, wenn man aktiv in der Politik ist – tief gehende Wirkungen auf den Arbeitsmarkt. Ich glaube nicht, dass in dieser Gesellschaft, durch wen auch immer, in einer absehbaren Zeit – und das hängt zusammen mit Informationstechnik – von Vollbeschäftigung die Rede sein kann, obwohl das alle Parteien in ihrem Programm fordern. Schätzungsweise in zwei Jahren wird mehr als die Hälfte der Arbeitsplätze wissensbasiert sein bei uns auf den unterschiedlichen Stufen. Und nun hören Sie sich bitte an, was der bedeutendste deutsche Soziologe, was Dahrendorf sagt, der, seitdem er englischer Lord ist, schon gar kein Blatt mehr vor den Mund nimmt. Ich zitiere ihn wörtlich: „Die Wissensgesellschaft erweist sich als Gesellschaft des bewussten Ausschlusses vieler aus der modernen Arbeitswelt." Das heißt, man kann die Arbeit, für die man früher hundert Leute gebraucht hat, heute mit 26 oder 10 machen. Man braucht für diese Arbeit Medien und Computerkompetenz und eine solide allgemeine Grundbildung. Und viele Menschen haben das entweder wegen Strukturmängeln unseres Bildungssystems oder aber aufgrund ihrer mangelnden Begabungen nicht. Das heißt, man muss sich darauf einstellen, dass wir einen polarisierten Arbeitsmarkt behalten, dass Computerunternehmen händeringend Einwanderungsgenehmigungen suchen für irgendwelche Leute aus der Ukraine oder aus Indien – und auf der anderen Seite haben wir 4.000.000 Arbeitslose. Und dies hat nun in der Tat eine sicherheitsrelevante Konsequenz, meine Damen und Herren. Ich fürchte, dies führt zu einer Gesellschaftsstruktur, die ich Zwei-Drittel-Gesellschaft nenne. Sie haben einen Zwei-Drittel-Block, der in unseren Breiten insgesamt gut verdient und gut leben kann. Aber sie haben ein Drittel von Leuten, die entweder keinen Job kriegen oder Downshifter, die sich der Grundtendenz unserer digitalen Ökonomie, der Beschleunigung nicht aussetzen wollen. Auch aus durchaus ehrenhaften Gründen: „Ich will mich nicht so hetzen." „Ich will mich um meine zwei Kinder kümmern."

Toleranz der Lebensstile ist notwendig. Aber, meine Damen und Herren, wie gehen wir dann gesellschaftlich und politisch mit diesem dritten Drittel um? Eins sage ich Ihnen: Wenn der Sozialstaat nicht mehr existiert oder so weit abgebaut wird, wie das in manchen vergleichbaren, technisch vergleichbaren Gesellschaften der Fall ist, dann bekommen Sie viel mehr Arbeit. Ich werde nie vergessen, wie ich das erste Mal nach Palo Alto kam – und das ist eine relativ kleine Stadt und eine Stadt, in der es ungeheuer viel Reichtum gibt. Trotzdem sagten mir die Leute: „Wenn du über die Brücke fährst, mach bitte die Türverschlüsse runter, damit die nicht von außen aufgemacht werden können oder halte nicht bei Rotlicht." Bisher konnten wir uns in den meisten europäischen Städten solche Viertel, wo dieses dritte Drittel und die unteren Segmente des dritten Drittels konzentriert sind, sparen. Das ist ein Zusammenhang zwischen Sozialpolitik und Sicherheitspolitik, den man nie vergessen sollte.

Herr Minister Schily hat mir erspart, über sicherheitspolitische Fragen im Detail zu sprechen. Denn er hat sie fast alle angesprochen. Ich halte auch keinen Vortrag über die Rasterfahndung und den Tatbestand, dass wir derzeit nicht überall, aber doch in wichtigen Medien, eine Rehabilitierung von Horst Herold feststellen können. Irgendwie sieht das ja anders aus, die Berichterstattung, als ich sie schon erlebt habe. Nein, ich will darüber gar nicht reden. Ich will Ihnen nur sagen: Es geht nicht allein um Technik. Man darf nicht allein auf Technik vertrauen, sondern muss sehen, dass es einen Zusammenhang gibt.

Ich mache Ihnen das an zwei ganz aktuellen Beispielen deutlich. Ich entnehme der Süddeutschen Zeitung folgenden Absatz: Selbst wenn islamistische Kämpfer etwa aus Tschetschenien nach getaner Arbeit nach Deutschland zurückkommen, ist aus ihnen kaum etwas herauszubringen. Wir haben hier einige Leute im Blickfeld, von denen wir hundertprozentig überzeugt sind, dass die in Tschetschenien waren, sagt ein Sicherheitsmann vor Ort. Aber da ist eine Wand, durch die kommen wir nicht durch. Und der Baden-Württembergische Verfassungsschutzexperte Herbert Müller sagt: Wir haben es mit lauter Biedermännern zu tun, mit Leuten, die keine Straftaten begangen haben, mit Leuten, die angeben, keiner Fliege etwas zuleide tun zu können, mit Leuten, die brav in die Moschee gehen – und jetzt wörtlich: „Mit Rasterfahndung ist da gar nichts zu machen", sagt Müller. Also offensichtlich kann es nicht nur auf Technik ankommen. Heute, sagt der Vorsitzende des Bundes der Kriminalbeamten, ist eine Rasterfahndung mit so weiten Kriterien wie bei uns wie Goldwaschen mit einem zu großen Sieb. Die Kriterien, die nach dem 11. September an die Täter angelegt werden, waren angeblich so vage, dass automatisch ein Großteil der moslemischen Bevölkerung in Deutschland darunter gefallen ist. Ich mache mir das nicht zu Eigen. Ich spiele hier nicht den Sicherheitsexperten. Ich sage nur: Es geht nicht um eine ganz bestimmte Technik, sondern es geht darum, wie diese Technik angewandt wird, was wir damit tun. Und insofern kann man nicht heilsbringend auf diese oder jene politische Einzelmaßnahme, diese oder jene Einzel-Technik schauen.

Man hat gelegentlich den Eindruck, dass die, die Verbrechen begehen und die man verfolgt und verfolgen muss, in einem Krieg mit den Sicherheitsleuten stehen, und manchmal scheinen sie auf klassische Instrumentarien auszuweichen trotz der modernen Technik. Ich höre die Vermutung, dass Usama Bin Laden und vergleichbare Leute gar keine Handys, geschweige UMTS-Handys, benutzen, sondern mit dem Mittel des Boten arbeiten, sozusagen mit Mitteln des alten Griechenland. Auch das ist eine Ausweichmöglichkeit. Die ist auch in diesem Bericht der Süddeutschen Zeitung angedeutet worden. Ich weiß, wie die Schwierigkeiten sind. Ich kenne die Klagen von manchen, die sagen: Wenn mal was passiert, dann fangen die in der Politik an, Veränderungen durchzuführen und durchzusetzen. Dann geht das plötzlich. Drei Jahre später oder zwei Jahre später ist das wieder alles vergessen. Ja, und dann kommt wieder die nächste Welle. Mag sein, dass das politische System insgesamt so reagiert. Es gibt auch Leute, die so kontinuierlich sind, dass sie gegen diese Wellen wirken. Einer davon ist hier im Saal. Aber, ich glaube, dass wir sehen müssen, dass es um dieses Dreieck, das der Präsident geschildert hat, geht und dass in diesem Dreieck die Interessen der drei unterschiedlichen Pole vernünftig miteinander abgeglichen werden müssen.

Da bin ich nun beim Thema „Sicherheit und Identitäten“ meine Damen und Herren. Ich nenne ein Beispiel: Aufgrund des Übertragungsmediums Funkwelle sind Funknetze besonders anfällig für Abhörangriffe. Die Verbreitung von Funkwellen lässt sich prinzipiell nicht beliebig einschränken. Und so ist es auch außerhalb des gewünschten Territoriums möglich, Funkkontakt zu einem W-Lan aufzubauen. Beim festverkabelten Netzwerk konnte man von außen nur durch Umgehung des schützenden Firewalls, durch physikalischen Zugriff auf das Kabel abgehört werden. Bei einem Funknetz reicht es wenigstens theoretisch, sich im Einzugsbereich eines Accesspoints zu befinden, wo mit geeigneten Maßnahmen Zugang zu erlangen ist. Aber es ist eine Tatsache, dass die Verbreitung von W-Lans in Deutschland ansteigt. Gleichzeitig sind zwei von fünf Unternehmensfunknetzwerken in Deutschland ungeschützt und damit besonders leicht angreifbar. Nach aktueller Rechtslage ist das Eindringen in ein solches ungeschütztes Netzwerk nicht einmal strafbar. Das ist wie das Lesen fremder Postkarten. Hacker müssen sich nur im Umkreis des Netzwerks bewegen, und schon können sie ungehindert Daten einsehen. Nur 11 % der Unternehmen planen, die Sicherheit drahtloser Netze durch Verschlüsselung kurzfristig auszubauen.

Schon bin ich bei der generellen Problematik. Ich habe vom dritten Drittel gesprochen. Das sind Leute, die eben nicht von früh bis abends in Arbeitsprozesse eingebunden sind. Auch nicht eingebunden sein wollen. Zum Beispiel gibt es deswegen die so genannten War Driver. Das sind Hacker, die mit einem für den Zugriff auf drahtlose Netzwerke ausgerüsteten Notebook in der Stadt herumfahren, um in Wireless Lans einzudringen. Wireless Lan-Hacker, die zu Fuß unterwegs sind, haben inzwischen ihre eigenen Gaunerzinken entwickelt, die sie mit Kreide an Bürogebäuden anbringen und die zum Beispiel zeigen, ob hier frei auf ein Netzwerk zugegriffen werden kann, ob es gesichert ist, welche Reichweite es hat usw. In der

Szene heißt das War Chalking, also von Chalk die Kreide. Was bedeutet das jetzt alles? Wenn die Lufthansa ihre Lounges mit W-Lans ausstattet, wenn die Deutsche Bahn W-Lan-Hotspots in Erster-Klasse-Lounges aufbaut, wenn T-Mobile bei Wireless Lan einsteigt – welche Art von „War" findet da statt? Und jetzt gehe ich weiter: Identitäten. Aus sozialpsychologischer Sicht ist das Selbst die Gesamtheit der auf die eigene Person bezogenen Inhalte. Sie wissen, welche Probleme ich anspreche. Mit Selbstwirksamkeit meint man den Grad des Überzeugtseins von der eigenen Handlungsfähigkeit. Es geht also um Fragen, wie sie in Sätzen, wie „So könnte ich werden.", oder „So möchte ich sein." zusammengefasst werden. Nun bin ich bei Online. Ich muss nicht sagen, dass die Frage, welche Identitäten wir entwickeln, wie wir sie darstellen, wie wir die Identitäten anderer Personen wahrnehmen, entscheidend von medialen Umgebungen abhängt. Ich rede jetzt nicht von den klassischen Massenmedien, die Sie alle kennen – denken Sie an Special-Interest-Zeitschriften, bei denen unterschiedliche Gruppenzugehörigkeiten kollektive Identitäten als Mann, Frau, Mädchen, Elternteil, Jäger, Kunstkenner, Körperschmuckträger, Surfer angesprochen werden. Das fängt schon mit Individualmedien wie Brief, Telefax, Festnetz, Mobiltelefon an. Man kann bei Brieffreundschaften, in Fankulturen kollektive Identitäten zum Ausdruck bringen. Das Medium hat über seinen Gebrauchswert hinaus symbolische Bedeutung und Zeichencharakter. Auch das ist etwas, was vom Sicherheitsstandpunkt aus analysiert werden kann und analysiert werden muss.

Und jetzt bin ich beim Problem „Netzmedien und Identitäten". Meine Damen und Herren, mit der Popularisierung des Internets sind Online-Selbstdarstellungen, digitale Identitäten, vor allem virtuelle Identitäten als neue Konstrukte im Umlauf. Leute benutzen Nicknames, mit denen sie sich selber charakterisieren. Sie anonymisieren die eigene E-Mail-Adresse. Sie treten als jemand auf, der sie gar nicht sind. Man kann durch die Nutzung eines Freemailers im World Wide Web anstelle des betriebseigenen E-Mail-Accounts bei der E-Mail-Adresse Anonymität herstellen. Also gibt es falsche Identitäten. Eine Bank, die feststellen will, ob der potenzielle Kunde volljährig und kreditwürdig ist, eine Frau, die wissen möchte, ob der oder die, die sie da anspricht, männlich, weiblich, homosexuell, heterosexuell, reich, arm, schwarz, weiß ist, die müssen digitales Identitätsmanagement betreiben. Ein Kollege von mir beschreibt es mit den Begriffen: Steuerung, wer welche personenbezogenen Daten der Fokusperson erhält und wie diese verwendet werden sollen sowie Darstellung, wer aktuell über welche personenbezogenen Daten der Fokusperson verfügt und wie diese tatsächlich verwendet werden bzw. welche Vereinbarungen bezüglich ihrer Verarbeitung bestehen. Ein ganzes Problembündel. Machen wir uns klar: Da über das Internet dank der Digitalisierung eine Fülle sozialer Treffpunkte und Foren zugänglich sind, die man zunächst unverbindlich und von den Mitmenschen unbeobachtet aufsuchen und zur sozialen Kommunikation nutzen kann, bietet sich die Chance, bewusst Netzszenarien auszuwählen, die bestimmten bevorzugten oder auch heiklen Identitäten weitere Ausdrucksmöglichkeiten verschaffen. Indem man eine bereits außerhalb

des Netzes etablierte Identität zusätzlich auch im Netz realisiert, erweitern sich die Möglichkeiten, soziale Bedürfnisse nach Information, Zugehörigkeit, Anerkennung, Unterstützung realistischer Selbsteinschätzung, Selbstwerterhöhung zu befriedigen. Das ist eine neue Form der Kommunikation, die wir vorher so nicht gekannt haben. Es sind auch neue Formen von Freiheit, die wir nicht nur aus Sicherheitsinteressen einschränken dürfen. Aber in der Tat entstehen hier Sicherheitsprobleme, die sich noch vergrößern, wenn die Zahl – ich rede von 2009 bis 2014 –, derer, die wirklich den Computer nicht nur als Schreibmaschine benutzen, sondern als Kommunikationsinstrument, wenn diese Zahl wirklich in die Millionen geht. Denn eins möchte ich Ihnen auf diesem Feld als Experte wirklich raten. Glauben Sie nicht diesen Zahlen von Forrester Research und all diesen Firmen über die hunderte Millionen von Internet-Nutzern. Die gibt es zwar. Das sind alle die, die einen Computer da stehen haben und die den irgendwann irgendwie nutzen. Aber nur eine Minderheit nutzt ihn als Kommunikationsapparat. Nun, meine Damen und Herren, in einigen Jahren werden ihn viele Millionen mehr als heute als Kommunikationsapparat nutzen mit all den unterschiedlichen Möglichkeiten, die es gibt. Und dann wird sich in der Tat das Problem auch für die Sicherheitspolitik erheblich verändern.

Ich gebe Ihnen ganz wenige Beispiele, die ich vor allem aus den Forschungen meiner Kollegin Sherry Turtle entnehme. Nehmen Sie nur das Beispiel MUDs, also Spiele, Multi User Dungeons, die auf verschiedener Software beruhen. MUDs setzen die Anwender in virtuelle Räume, in denen man navigieren, kommunizieren, konstruieren kann. Also wenn ich zum Beispiel eine Figur „Esther" spiele, dann erscheinen sämtliche Wörter, die ich nach dem Befehl „Say" eingebe, auf dem Bildschirm aller Spieler als „Esther says". In einigen MUDs werden die Spiele durch Piktogramme repräsentiert. Das meiste ist aber textgeschützt. Und nun sage ich Ihnen noch, was mit den Menschen passiert. Sherry Turtle erzählt von Duck, Collegestudent mittlerer Westen, er spielt vier Rollen in drei verschiedenen MUDs. Eine ist die einer verführerischen Frau. Eine andere ist die eines Machos. Die dritte Figur ist die eines geschlechtsgetreuen Hasen namens Garret, der durch seine MUD schlendert und Leute miteinander bekannt macht. Drei unterschiedliche Rollen – ein Collegestudent. Im Übrigen, es gibt auch Collegestudenten, die sieben oder acht Stunden am Tag im Netz sind. Wenn jemand zwölf Stunden als Börsenmakler tätig ist, sagen wir: Das ist ein toller Mensch. Wenn er aber so lange im Netz ist, sagen wir: Er ist süchtig. Meine Damen und Herren, was tut sich da? Ich sage Ihnen, was dieser Duck sagt. Das ist zitiert nach Sherry Turtle. „Ich spalte mich auf." Das gelingt mir immer besser. Indem ich mich selbst als zwei, drei oder mehr – also als jemanden betrachte, der von einem Fenster zum anderen wechselt, aktiviere ich jeweils einen anderen Teil meiner Persönlichkeit. Während ich in einem Fenster eine Art Streitgespräch führe, versuche ich mich im MUD eines anderen Fensters an ein Mädchen ranzumachen, während woanders ein Tabellenkalkulationsprogramm läuft. Dann erhalte ich eine Echtzeitmeldung, die auf dem Bildschirm erscheint, sobald sie von einem anderen Systembenutzer

abgeschickt wurde. Und ich vermute, dass es Real Life ist. Und dann sagt dieser Student den Satz, den ich Sie bitte mitzunehmen. „Real" Life ist nur ein Fenster unter vielen, und es ist gewöhnlich nicht mein bestes. Wir reden über die Frage, was eigentlich wirklich diese moderne Informations- und Kommunikationstechnik verändert. Stimmen Sie mir zu, dass die Welt sich verändert, wenn es immer mehr Menschen, zum Beispiel aus dem dritten Drittel geben sollte, die sagen, dass Real Life nicht mehr ihr bestes Fenster sei?

Ein anderes Beispiel bezieht sich auf die Sexualität. Es ist ja mehrfach von Kinderpornographie die Rede. Jetzt rede ich mal von anderen Formen von Sexualität. Ronald, ein Mathematikstudent in Memphis, nennt sich Backslash und tippt ein „Emote", streichelt Targas Brust und sagt: „Du bist schön Targa." Elizabeth, die Person hinter Targa, antwortet mit: „Berühr mich noch einmal, aber fester. Bitte jetzt gleich. So mag ich's." Sherry Turtle kommentiert das mit den Sätzen: „Einvernehmliche Beziehungen sind nur eine Facette des virtuellen Sex. In MUDs kann es zu virtuellen Vergewaltigungen kommen, wenn ein Spieler einen Weg findet, die Handlungen der Figur eines anderen Spielers zu kontrollieren und so auch diese Figur zum Sex zu zwingen. Zwang wird immer dann ausgeübt, wenn ein Spieler die Aktionen und Reaktionen von Figuren unabhängig von den Wünschen ihrer Spieler steuern kann. Wenn Ronald ein solcher Schurke wäre, dann würde nur er für die Figur Targa Anweisungen eingeben. In diesem Fall würde Elizabeth, die Targa spielt, an ihrem Computer sitzen und schockiert feststellen, dass sie selbst beziehungsweise ihr Selbst Backslash um zudringliche Zärtlichkeiten und schließlich um gewaltsamen Geschlechtsverkehr bittet."

Ich erspare Ihnen die vielfältigen postmodernen Thesen über multiple und flexible Ichs. Ich will nur sagen: diese digitalen Medien erlauben den Menschen eine Vielfalt und Flexibilität, wie wir sie bisher nicht gekannt haben. Im Prinzip ist das positiv. Es gab aber auch die negativen Rückwirkungen, die heute im Vortrag von Bundesminister Schily geschildert wurden. Manche Leute schließen daraus, dass sich die „Selbste" als Konstrukte entlarven, die Menschen könnten ihre verschiedenen „Selbste" gar nicht mehr zusammenhalten. Ich halte das für philosophische Spielereien. Aber dass sich da etwas verändert mit den Menschen, für die Sie Sicherheit garantieren sollen, daran kann kein Zweifel sein. Und das hängt nicht nur mit Rasterfahndung und mit der Technik zusammen, über die gleich anschließend ein Kollege sprechen wird. Bilder verführen. Bilder können reicher und faszinierender sein als das wirkliche Leben. Es gibt Menschen, die Gefangene ihrer Bildschirme sind. Wir können in virtuellen Welten verloren gehen. Unsere Gesellschaft, will ich am Schluss sagen, muss sich um solche Fragen kümmern. Die Zeiten, in der praktisch jeder, der nicht verhungern wollte, den ganzen Tag mit der Erwerbsarbeit verbringen wollte, sind vorbei. Wenn wir ein Drittel der Menschen haben, die entweder an die Erwerbsarbeit nicht herangelassen werden oder der Erwerbsarbeit ausweichen können, mit welchem Patchwork-Einkommen auch immer, für die bekommen die Ersatzwelten, die ich Ihnen gerade dargestellt habe, eine immer größere Bedeutung. Und jetzt füge ich hinzu – das ist eher an die Wirt-

schaftscommunity in diesem Dreieck gerichtet, aber trotzdem sage ich es –: Wenn wir eine Leistungsgesellschaft, eine Gesellschaft mit hohem Bruttosozialprodukt, eine Gesellschaft mit stetigem Wachstum bleiben wollen, brauchen wir eine genügende Anzahl von Menschen, die den ökonomischen Apparat bedienen und die bereit sind, in diesem Zweidrittelblock unter dem Gesetz der Beschleunigung zu arbeiten. Oder anders gesagt: Dann darf es nicht zu viele Leute geben, die das sagen, was der in meiner Community, in meinem Job berühmteste Witz sagt. „Someone got my social security number of the Internet and stole my identity. Thank god. I hate it being me."

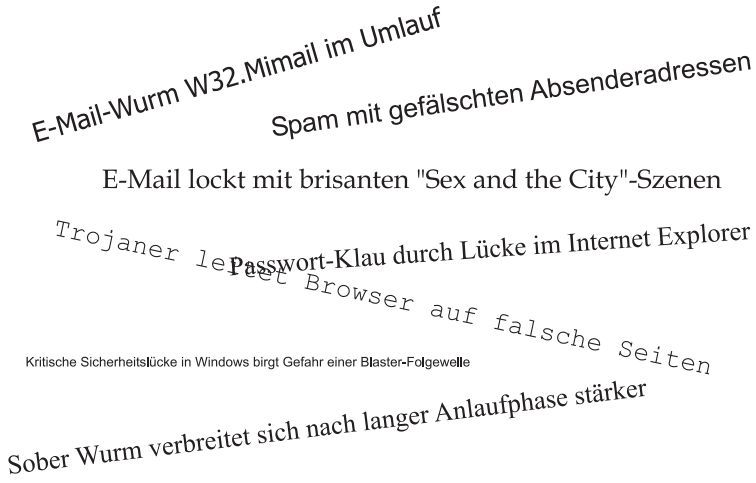
Lage, Bedrohungsszenarien und Handlungsbedarf

Max-Peter Ratzel

Dieser Tage wird in Genf der erste „World Summit on the Information Society“ (Weltgipfel über die Informationsgesellschaft) durchgeführt, zu dem etwa 6.000 Teilnehmer erwartet werden. Vertreter von Regierungen, der Wirtschaft und von Nichtregierungsorganisationen werden teilnehmen. Einige Dutzend Staats- und Regierungschefs haben ihre Teilnahme zugesagt. Bundeskanzler Schröder wird die deutsche Delegation anführen. Dies belegt eindrucksvoll die geopolitische Bedeutung des Themas. Die Industriestaaten wandeln sich von der Industrie- zur Informationsgesellschaft; PR Dr. Kersten hat dies bereits in seiner Begrüßungsansprache ausgeführt.

Max-Peter Ratzel, Abteilungspräsident im BKA, berichtete über die aktuelle Lage

Internet, E-Mail, e-commerce sind Begrifflichkeiten, die sich mittlerweile auch im alltäglichen Sprachgebrauch etabliert haben. Digitale Daten und der digitale Versand von Informationen sind ein essentieller Bestandteil des öffentlichen wie des privaten Lebens. Die Vorteile dieser Entwicklung sind unbestritten. Die schnelle Verfügbarkeit von Informationen und die einfache globale Kommunikation mittels Internet eröffnen neue Chancen für die wirtschaftliche und gesellschaftliche Entwicklung. Die Möglichkeiten der modernen Medien sind bei weitem noch nicht ausgeschöpft. Dies ist die gesellschaftspolitische Dimension der Thematik.



Naturgemäß haben auch Straftäter die Möglichkeiten der Nutzung von Informations- und Kommunikationstechnik als Tatmittel für die Begehung von Straftaten entdeckt. Die einzelnen Straftaten können einerseits schneller oder geschickter begangen, andererseits besser camoufliert werden. Hinzu kommt, dass die Informations- und Kommunikationstechnik mittlerweile ein wesentliches Element der globalen Zusammenarbeit darstellt und somit selbst Ziel von Angriffen wird. Die hier gezeigten Veröffentlichungen skizzieren einen Teil des Szenarios. Meldungen wie diese zeigen die Notwendigkeit einer umfassenden Darstellung und Analyse von Straftaten unter Nutzung der Informations- und Kommunikationstechnik (IuK) sowie von Angriffen gegen IuK-Strukturen auf. Erkennbar werden aber auch Handlungsnotwendigkeiten für Polizei, Justiz und andere Beteiligte. Damit erschließt sich auch die sicherheitspolitische Dimension des Themas.

Kriminalistisch unterscheidet man im Bereich IuK-Kriminalität zwischen herkömmlichen Straftaten, bei denen die IuK als Tatmittel eingesetzt wird, und Straftaten, bei denen die IuK selbst Ziel des Angriffs ist.

Beispielhaft für die Nutzung der IuK als Tatmittel ist die Verbreitung von Kinderpornografie in Datennetzen. Für die Variante IuK als Tatziel steht das so genannte Hacking, das Eindringen in fremde Rechner oder Datennetze mit dem Ziel der Sabotage.

Ich werde mich nachfolgend auf Aspekte konzentrieren, die mit der Funktion der IuK als potenziellem Tatziel zusammenhängen. Hierbei handelt es sich um IuK-Kriminalität im engeren Sinne. Eintrittswahrscheinlichkeit wie auch potenzielle

Schadenshöhen oder -auswirkungen erfordern eine besonders sensible Betrachtung dieses Teil-Phänomens.

„Lage, Bedrohungsszenarien und Handlungsbedarf“

Lageskizzierung

Bei einer ersten Betrachtung der polizeilichen Kriminalstatistik 2002 wird deutlich, dass die Fallzahlen im Bereich der IuK-Kriminalität, bezogen auf die Gesamtkriminalität in Deutschland, gering scheinen.

In der IuK-Kriminalität besteht ein besonders hohes Dunkelfeld, teils auf Grund von Unkenntnis, teils aus mangelndem Interesse an der Strafverfolgung seitens der Betroffenen. Die Anzeigebereitschaft ist zurückhaltend. Dies gilt vor allem für Wirtschaftsunternehmen. Diese befürchten aus nachvollziehbaren Gründen Image- und Vertrauensverluste, wenn sie sich gegenüber der Polizei oder gegenüber ihren Partnern und Kunden öffnen.

Zwei gegenläufige Entwicklungen sind erkennbar – Innenminister Schily hat dies bereits in seinem Eröffnungsvortrag herausgestellt. Einerseits ist nach Jahren kontinuierlich steigender Zahlen im Jahr 2002 erstmals eine insgesamt rückläufige Tendenz zu verzeichnen.

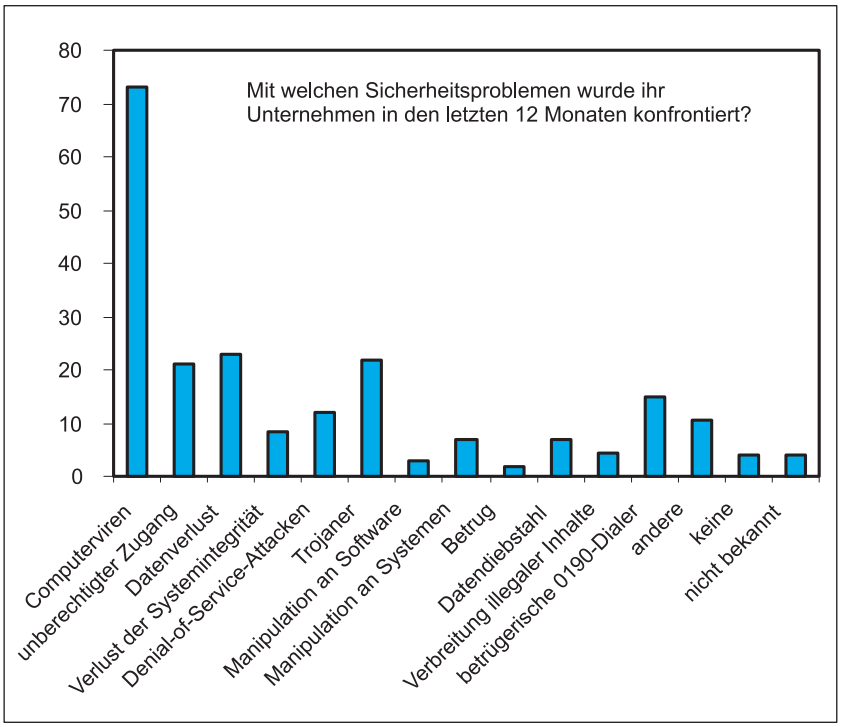
Dem gegenüber steht aber ein Anstieg des Fallaufkommens um mehr als 50 % bei einzelnen Delikten, wie „Datenveränderung“ und „Computersabotage“. Dies sind Straftaten mit einer besonderen Qualität. Auch die Fallzahlen der gewerbsmäßigen Softwarepiraterie sind von 2001 auf 2002 deutlich angestiegen.

Die Zahlen, untermauert durch weitergehende Erkenntnisse der IuK-Fachdienststellen, verdeutlichen, dass neue, qualifiziertere Erscheinungsformen der IuK-Kriminalität zunehmen.

Zwar hält sich etwa die Zahl der festgestellten und meist hochspezialisierten Täter beim Phänomen Hacking in Grenzen, aber die potenziellen Schadenshöhen sind auf Grund deren umfangreicher Kenntnisse über die Technik und die ihr immanenten Schwachstellen immens. Oftmals sind die Täter selbst in der Branche tätig und somit auf dem gleichen Wissensstand wie Administratoren und IT-Sicherheitsfachleute. Dieses Verhältnis stellt für die Prävention wie für die Repression eine besondere Herausforderung dar.

Ich darf eine Studie der renommierten Unternehmensberatung PriceWaterhouseCoopers (PWC) zitieren, wonach bei einer Befragung von Unternehmen zu Sicherheitsproblemen über 70 % die Existenz von Computerviren in ihren IT-Systemen eingeräumt haben. Als vermutete Ursache wurde zu 36 % das Ausnutzen bekannter Schwachstellen im Betriebssystem angegeben.

„Lage, Bedrohungsszenarien und Handlungsbedarf“



Als Verursacher wurden zu knapp 42 % Hacker genannt, jedoch zu mehr als 52 % autorisierte oder nicht autorisierte Benutzer/Mitarbeiter. Deshalb müssen nicht

nur Sicherheitsmechanismen nach außen gestärkt, sondern auch im Innenbereich entsprechende Sicherheitsmaßnahmen forciert werden.

Die Zahlen belegen exemplarisch die hohe Verbreitung von Angriffen gegen Computersysteme, aber auch den nach wie vor zu geringen Sicherheitsstandard zur Abwehr solcher Angriffe.

Gerade bei der Abwehr von Angriffen auf die IuK ist die Täter-Typologie für alle Beteiligten ein wesentlicher Ansatzpunkt präventiver Maßnahmen. Nach Erkenntnissen des BKA wie auch nach Einschätzung namhafter Experten kann der Kreis der in Frage kommenden Tatverdächtigen für den Phänomenbereich Hacking wie folgt umrissen werden:

- Innentäter
  - bewusst handelnde Täter
  - Mitarbeiter ohne ausreichende fachliche Qualifikation oder mit mangelndem Sicherheitsbewusstsein
- Außentäter
- Hacker „aus Neugier“
- Hacker „mit professioneller Ausrichtung“
  - Terroristen oder staatliche Organisationen

Die Lageskizzierung und der Hinweis auf die unterschiedlichen Tätertypologien verdeutlichen, dass sich hier ein neues Gefahrenpotenzial entwickelt, dem sich neben den IT-Entwicklern und IT-Betreibern auch die Strafverfolgungsbehörden frühzeitig und angemessen widmen müssen.

Aktivitäten des BKA

Aufgaben des BKA

Lassen Sie mich auf die Schwerpunkte, die das BKA im Bereich der IuK-Kriminalität setzt, näher eingehen. Dazu ist zunächst ein kurzer Exkurs zu den Aufgaben des Bundeskriminalamtes sinnvoll:

Das Bundeskriminalamt wertet als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei alle relevanten Informationen zur IuK-Kriminalität aus und stellt die Ergebnisse den Polizeien der Länder für repressive wie auch für präventive Zwecke zur Verfügung. Daneben unterstützt es die Polizeien der Länder in der praktischen Fallarbeit (Datensicherung, -sichtung und -auswertung) sowie in der kriminalpolizeilichen Fortbildung.

Im Übrigen tauscht das BKA seine Informationen und Erkenntnisse auch mit den Zentralstellen anderer Staaten sowie im Rahmen bi- und multilateraler Arbeitsgruppen oder -gremien (Interpol, Europol, G 8 etc.) aus.

Daneben ist das Bundeskriminalamt als Kriminalpolizei des Bundes originär für die Strafverfolgung in Fällen von Straftaten nach § 303 b StGB verantwortlich,

soweit tatsächliche Anhaltspunkte dafür vorliegen, dass die Tat entweder gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder gegen so genannte „kritische Infrastrukturen“ gerichtet ist. Diese Zuständigkeitsregelung ist auf den ersten Blick auf Repression ausgerichtet. Aber in jeder Strafverfolgung liegen neben spezialpräventiven Aspekten auch generalpräventive Gesichtspunkte.

Ermittlungsverfahren

Ich will an dieser Stelle auf einige Details im Zusammenhang mit dem bereits von Minister Schily erwähnten Ermittlungsverfahren des BKA wegen Verdachts des gewerbsmäßigen Betruges sowie Verstößen gegen das Marken- und Urheberrecht eingehen. Dieses Verfahren hat vor etwa drei Wochen in den Medien große Beachtung gefunden. Minister Schily hat die Dimension dieses Ermittlungsverfahrens bereits herausgestellt.

Die Maßnahmen richteten sich gegen mehrere Beschuldigte, die im Verdacht stehen, Computersoftware betrügerisch in den Handel gebracht zu haben. Geschädigt waren in diesem Fall nicht nur die Firma Microsoft und andere Softwarehersteller, sondern vor allem legal operierende Marktkonkurrenten sowie Endverbraucher. Diese haben gutgläubig Software-Produkte eingekauft, die sie aus heutiger Sicht unberechtigt verwenden.

Gegen den Hauptbeschuldigten waren bereits in der Vergangenheit durch verschiedene Staatsanwaltschaften Ermittlungsverfahren wegen des Verdachts von Urheberrechtsverletzungen geführt worden. Diese Verfahren endeten entweder mit der Einstellung oder mit Strafbefehlen, deren Vollstreckung zur Bewährung ausgesetzt wurden. Bis dato wurden keine Ermittlungen wegen gewerbsmäßigen Betruges geführt. Insbesondere wurden keine Finanzermittlungen oder vermögensabschöpfende Maßnahmen initiiert. Die derzeit vom BKA im Auftrag der StA Bochum geführten Ermittlungen haben genau diese Maßnahmen jedoch von Anfang an beinhaltet.

Nach konservativen Schätzungen gehen wir von einem finanziellen Schaden aus, der bei mindestens 16 Millionen Euro liegt; Microsoft unterstellt gar einen Schaden in dreistelliger Millionenhöhe. Nicht berücksichtigt in diesen Schadenssummen sind die materiellen wie immateriellen Schäden. Diese sind durch Insolvenzen von Mitbewerbern eingetreten, die dem wirtschaftlichen Druck der Betrüger naturgemäß nicht standhalten konnten.

Eine besondere Herausforderung stellt die Auswertung der umfangreichen Asservate dar. In diesem Verfahren sind es etwa 60 Kubikmeter. Bei deren Auswertung sind drei verschiedene Zielrichtungen zu unterscheiden:

– Beweismittel im Strafverfahren (z. B. gefälschte Software),

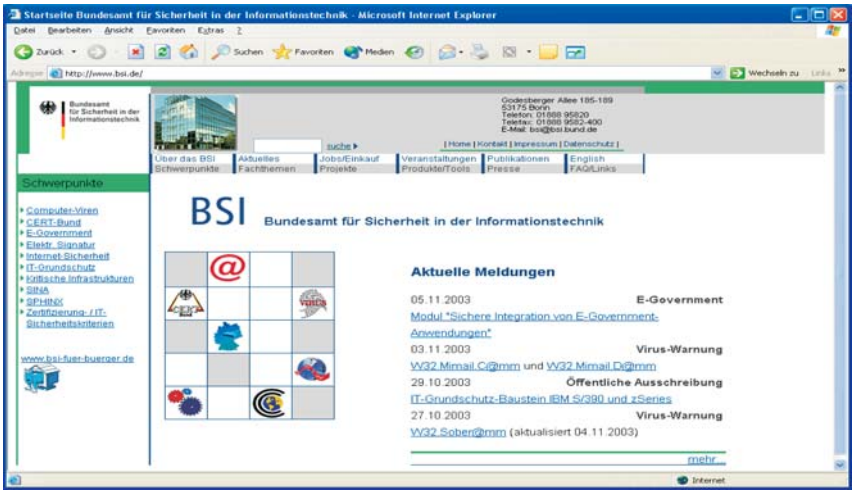
– beabsichtigte Einziehung als Tatmittel (z. B. zur Fälschung verwendete Gegenstände) sowie
– Pfändung im Rahmen der vermögensabschöpfenden Maßnahmen (Vermögenswerte, z. B. auch echte Softwareprodukte als Betriebsvermögen).

Diese Fakten zeigen die Herausforderungen, denen Polizei und Justiz bei der Führung eines solchen Verfahrenskomplexes gegenüberstehen. Es bleibt abzuwarten, welche Früchte die Ermittlungen noch tragen werden.

Hacking-Prävention

Ein weiteres Tätigkeitsfeld des BKA ist die Verfolgung von **Hacking-Angriffen**.

Unter Hacking versteht man das unbefugte Eindringen in geschlossene Computersysteme. Hierbei ist unser Augenmerk sowohl auf das Verbreiten von Viren, Würmern und Trojanern gerichtet, als auch auf Denial of Service (DOS)-Attacken oder das unautorisierte Umkonfigurieren von Administratorenrechten. Bei diesen Angriffen wird beispielsweise ein Netzwerk durch eine unüberschaubare Zahl von Anfragen mit dem Ziel des Teil- oder Totalausfalls belastet.



Es vergeht kaum eine Woche, in der nicht durch eine der Anlauf- und Beratungsstellen für Computernotfälle, die so genannten „computer emergency response teams“ (CERT), oder durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor neuen gefährlichen Entwicklungen gewarnt wird.

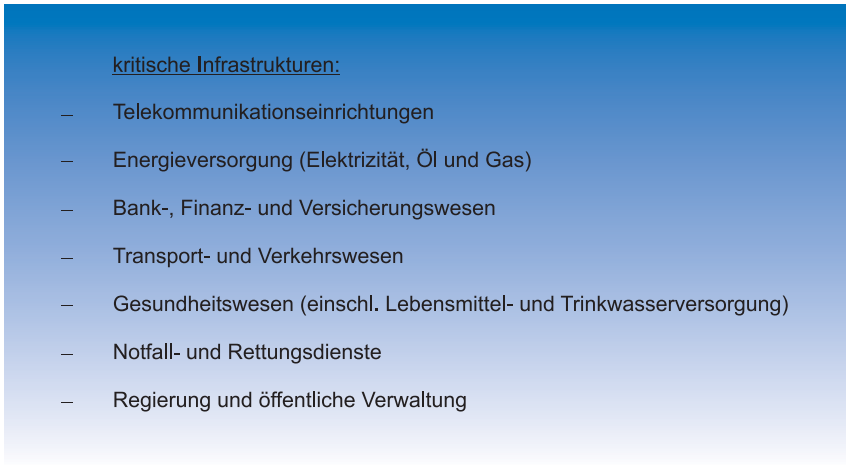
Im letzten Jahr hat die Zahl der Angriffe mittels „elektronischem Ungeziefer“ deutlich zugenommen. Dabei divergieren die geschätzten Schadenssummen stark.

Das BKA unternimmt große Anstrengungen, um die Strafverfolgung von Hacking-Angriffen zu gewährleisten, sei es

– bei der Sicherung und Auswertung von beschlagnahmten Datenträgern,
– bei der Beschaffung notwendiger Informationen im In- und Ausland oder
– durch die Führung von Ermittlungsverfahren in eigener Zuständigkeit.

Wir bemühen uns insbesondere um eine effektive Fallbearbeitung auf dem Gebiet „Hacking kritischer Infrastrukturen“. Unter kritischen Infrastrukturen verstehen wir Einrichtungen mit (lebens)wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Störung für größere Bevölkerungsgruppen nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten.

„Lage, Bedrohungsszenarien und Handlungsbedarf“



Dies sind im Einzelnen:

- Telekommunikationseinrichtungen
- Energieversorgung (Elektrizität, Öl und Gas)
- Bank-, Finanz- und Versicherungswesen
- Transport- und Verkehrswesen
- Gesundheitswesen (einschließlich Lebensmittel- und Trinkwasserversorgung)
- Notfall- und Rettungsdienste
- Regierung und öffentliche Verwaltung

Um den Anforderungen im Bereich des Schutzes kritischer Infrastrukturen entsprechen zu können, bedarf es umfassender Anstrengungen. In einem eigens dazu aufgelegten Projekt werden die spezifische Verwundbarkeit von Systemen und daraus entstehende Risiken untersucht. Ziel ist es, Schwachstellen aufzude-

cken, Bedrohungsszenarien zu erarbeiten und daraus Handlungsempfehlungen zur Gefahrenvermeidung abzuleiten.

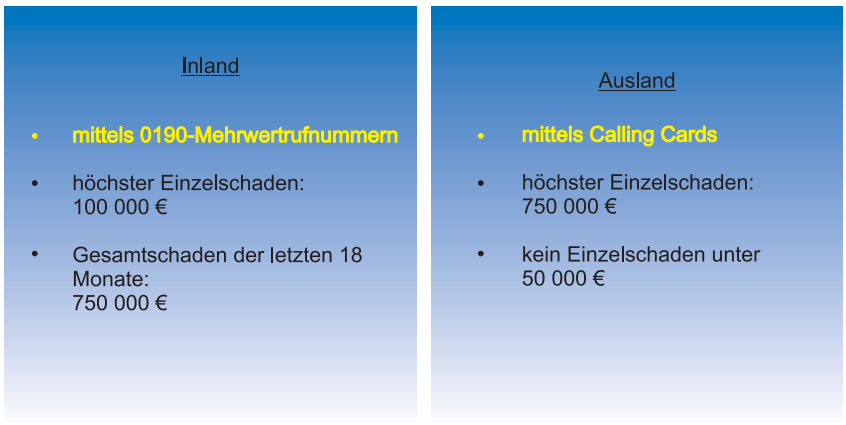
Phreaking

Ein neuer Schwerpunkt in der Wahrnehmung der Zentralstellenfunktion des BKA ist die Bekämpfung der **missbräuchlichen Verwendung von Telekommunikations-Anlagen**. Diese Art des Computerbetruges wird als **„Phreaking“** (Phone break in) bezeichnet. Dahinter verbirgt sich ein modus operandi, bei dem Personen unberechtigt auf Telefonanlagen von Firmen zugreifen und durch intensive Nutzung, zum Beispiel von Überseeverbindungen, hohe Kosten verursachen. Oder es kommt zu Gesprächsverbindungen über die Telefonanlagen der Firmen, bei denen die Täter 0190-Mehrwertdienste anwählen, die sie zuvor auf ihren Namen oder auf Strohleute registriert haben.

Inlands- und Auslandstaten ergänzen sich in verschiedener Hinsicht, allen sind hohe Schäden immanent. Die anfallenden Telefonkosten sind in Einzelfällen für die Firmen existenzbedrohend.

„Lage, Bedrohungsszenarien und Handlungsbedarf“

Schadenssummen Phreaking



Das BKA ist hier insbesondere in der nationalen und internationalen Koordination sowie in der Sicherung und Auswertung beschlagnahmter Datenträger aktiv. So wurde in diesem Jahr ein Personengeflecht aufgedeckt, das bundesweit Telefonanlagen penetrierte und dadurch immense Schäden verursachte. Eine größere Tätergruppe verursachte beispielsweise durch das Manipulieren von Telefonanlagen namhafter, in Deutschland ansässiger Unternehmen in den letzten 18 Monaten einen Gesamtschaden von 750.000 €.

Es ist anzunehmen, dass dies nur ein Bruchteil des tatsächlichen Schadens ausmacht. Wir gehen auf Grund des Anzeigeverhaltens der Firmen davon aus, dass auf diesem Sektor ein erhebliches Dunkelfeld existiert.

Zusätzlicher Schaden entsteht durch Straftaten in europäischen Nachbarländern. Dort werden Rufnummern von Telefonanlagen deutscher Firmen auf so genannte „calling cards" gespeichert und vertrieben. Für einen geringen Obolus können die Karten auf dem Schwarzmarkt erworben und für Telefonate in andere Staaten genutzt werden. Nach unseren Erkenntnissen telefonierten in einem Fall zahlreiche Calling-Card-Käufer gleichzeitig über eine einzige Telefonanlage. Der Schaden betrug alleine in einem Fall 400.000 €.

Auch der **missbräuchlichen Verwendung von 0190er Dialerprogrammen** gebührt eine besondere Beachtung.

Dialerprogramme, eigentlich als Abrechnungsmöglichkeit von Kleinstbeträgen im Internet geschaffen, symbolisieren mittlerweile eine der kriminellen Schattenseiten bei der Nutzung des Internet. Sie installieren eine ungewollte DFÜ-Verbindung auf dem PC, die sich oft unbemerkt über eine 0190er-Mehrwertrufnummer ins Internet einwählt und somit überhöhte Telefonkosten beim Geschädigten verursacht.

Hier ist das BKA insbesondere als deutsche Interpoldienststelle gefragt, da viele der tatverdächtigen Firmen und Personen im Ausland ansässig sind. Die mittlerweile eingeführten gesetzlichen Maßnahmen müssen hinsichtlich ihrer Auswirkungen auf dieses Kriminalitätsphänomen evaluiert werden.

Bedrohungsszenarien

Neben diesen Fallschilderungen, die im Wesentlichen zu materiellen Schäden führen, gibt es aber weitaus bedrohlichere Szenarien. Lassen Sie mich das Problem pointieren:

- Was passiert, wenn es Hackern gelingt, in die Computeranlage eines Energieerzeugers einzudringen?
- Welche Folgen entstehen, wenn die Software der Deutschen Bahn AG zur Steuerung der Gleisanlagen verändert wird?

Könnten dies tunliche Angriffsziele sein? Wenn ja, für welchen Täterkreis?

Schnell fallen in diesem Zusammenhang die Schlagwörter „Cyberterrorismus", „Cyberwar" oder „Informationskrieg". Gelegentlich werden die Begriffe synonym verwendet. In anderen Zusammenhängen sind sie weit gefasst und bewusst unscharf gehalten. Eine konsentierte Definition gibt es bislang nicht. Sind diese – geradezu apokalyptisch klingenden – Begriffe richtig gewählt? Wird damit nicht – ohne realen Hintergrund – Panikmache betrieben? Dies sind Fragen, die aus polizeilicher beziehungsweise forensischer Sicht derzeit kaum zu beantworten sind. Lassen Sie mich etwas detaillierter auf dieses Problem eingehen.

Nach einer Begriffsbestimmung Alexander Siedschlags von der Humboldt Universität Berlin werden Cyberwarfare und Cyberterrorismus als Handlungen gegen Informationssysteme oder Digitaltechnik definiert, wobei Cyberwarfare staatliches Handeln bezeichnet.

„Cyberterrorismus ist politisch motiviertes Hacken, das zum Ziel hat, ernsthaften Schaden anzurichten" – so lautet die Definition nach D. Denning, Professorin für Informatik an der Georgetown Universität in Washington.

Lassen Sie mich mittels eines authentischen Beispiels, anhand dessen man einen Einblick in die Verknüpfungen zwischen kritischen Infrastrukturen und destruktiven Angriffen bis hin zum möglichen „Cyberterrorismus" bekommen kann, das Gefahrenpotenzial erläutern.

Root-Server und Virus-Infektion

Als am 21. 10. 2002 sieben der 13 weltweit installierten Root-Server des Internet ihren Betrieb aufgrund eines Hackingangriffes einstellten und zwei weitere in ihrer Leistungsfähigkeit eingeschränkt waren, kam es im Internet zu erheblichen Schwierigkeiten für die Nutzer.

Diese Root-Server stehen am Beginn einer Hierarchiekette. Sie ermöglichen eine Identifizierung der hinter den IP-Adressen „verborgenen" Domaine-Namen. Fällt diese Funktionalität aus, weiß ein Rechner beispielsweise nicht, welche IP-Adresse sich hinter www.bka.de verbirgt. Damit kann man die homepage des BKA nicht mehr erreichen.

Der dahinter stehende modus operandi des Angriffes ist eine so genannte „distributed denial of service" (DDOS) – Attacke. Diese belastet das System durch eine große Zahl von Anfragen. Dieser Belastungsanstieg führt in Folge zu einem Ausfall des Systems.

Durch ein solches Handeln entsteht den Tätern weder ein geldwerter Vorteil noch ein Zuwachs von Informationen. Es ist ein rein destruktives Handeln. Trotzdem ist es nicht möglich, allein auf Grund der Tatausführung einen politischen Hintergrund zu erkennen oder zu unterstellen. Das Überschreiten der Grenze zwischen Computersabotage und „Cyberterrorismus" ist erst dann zu erkennen, wenn man die Motivation der Täter erkennen oder begründet vermuten kann.

SPIEGEL-Artikel

Dass die zur Begehung derartiger Straftaten erforderlichen Informationen nicht ausschließlich in Fachkreisen verfügbar sind, zeigt ein Bericht des Nachrichtenmagazins „DER SPIEGEL" in seiner Ausgabe 32/2003. Dort wurde über die Dissertation eines US-Studenten zu verwundbaren Stellen in Glasfaser-Netzwerken berichtet. Bei Veröffentlichung dieser Erkenntnisse hätten sachkundige Straftäter

ausreichende Zugriffs- und Nutzungsinformationen erhalten, um unüberschaubare Szenarien Wirklichkeit werden zu lassen. Als Folge dieser Risikoeinschätzung wurde die Veröffentlichung der Dissertation untersagt.

SQL-Slammer

Aber auch andere Szenarien sind denkbar. Ich darf hier nur kurz auf den so genannten SQL-Slammer vom Januar 2003 hinweisen. Ende Januar 2003 wurde der Wurm SQL-Slammer erstmals registriert. Dabei handelte es sich um den Wurm mit der bislang höchsten Ausbreitungsgeschwindigkeit. In nur zehn Minuten verbreitete er sich weltweit und verdoppelte die Anzahl der infizierten Rechner alle 8,5 Sekunden. In seiner aktivsten Phase, etwa drei Minuten nach Beginn der Epidemie, scannte er das Netz mit einer Last von 55 Millionen IP-Adressen pro Sekunde. Der Wurm verursachte nach Angaben der britischen Marktforschungsfirma mi2 g „vergleichsweise niedrige Ausfallkosten“ von rund einer Milliarde US-Dollar.

Dieser Fall ist ein Angriff auf die Verfügbarkeit und Performanz des Internet selbst. Dafür spricht, dass der Wurm durch seine eigene Verbreitung derart enorme Datendurchsätze in der Netzstruktur verursachte, dass das Internet als solches phasenweise nicht mehr verfügbar war. Darüber hinaus hatte der Wurm keine unmittelbar wirksam werdende, individuelle Schadensfunktion.

Zu dem oder den Tätern können bislang keine verlässlichen Einschätzungen getroffen werden, vermutlich handelt es sich um so genannte „script kiddies“.

Begünstigt wurde die Verbreitung des Wurms aber auch durch mangelndes Verantwortungsbewusstsein der IT-Branche und der Nutzer. Eine seit Monaten existierende Software zum Schließen dieser bekannten Sicherheitslücke hätte nur rechtzeitig eingespielt werden müssen.

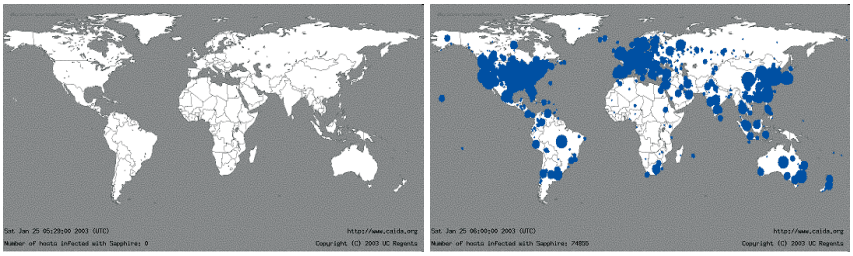
Derartige Fallbeispiele verdeutlichen die Abhängigkeit unseres Alltagslebens von der IuK und deren Anfälligkeit. Gerade die Verbindung zwischen kritischen Infrastrukturen und Informationstechnik wird auch in Zukunft ein Brennpunkt des Interesses bleiben. Oftmals ist uns die Dimension dieser Verknüpfung nicht bewusst.

Spezialisten des TÜV Rheinland testeten kürzlich Telefonanlagen mittels eines speziell entwickelten Tools auf Sicherheitslücken. Beim Scannen der Nebenstellen einer Telefonanlage entdeckten sie eine Rufnummer, hinter der sich ein Modem befand. Sie wählten sich über dieses Modem in die Telefonanlage ein. Möglich war dies, da nur unzureichende Sicherungseinstellungen vorhanden waren.

Im konkreten Fall war das Modem der Fernwartungszugang einer Firma, welche die Klimaanlage des Unternehmens auf diesem Wege administrierte und wartete. Somit hätten potenzielle Eindringlinge die Möglichkeit gehabt, Einstellungen an

der Anlage zu verändern und somit auch sensible Bereiche des Unternehmens lahm zu legen.

Ausbreitung des W32/qlslammer innerhalb der ersten 30 min



hohe Geschwindigkeit auf Grund der geringen Größe (1/10 des Wurms „Code Red“) und der hohen Leistungsfähigkeit der angegriffenen Ziele (SQL-Server)

Jedoch werden auch die klassischen Angriffsszenarien nicht ohne weiteres zurückgehen. Grund hierfür ist die hohe Verfügbarkeit von entsprechenden Programmen, ungesicherten Computersystemen sowie allgemein einer unzureichenden Sensibilisierung für notwendige Präventionsmaßnahmen.

Besonders sensible und öffentlichkeitswirksame IT-Systeme werden von Tätern immer wieder als geeignete Tatobjekte angesehen und – abhängig vom Grad der eingesetzten Sicherheitsmechanismen – angegriffen werden.

Beispielsweise zählte das Pentagon in den ersten sieben Monaten des Jahres 2000 etwa 14.000 Hacking-Attacken gegen die eigenen IT-Systeme.

Diese Beispiele zeigen auf, welche wirtschaftlichen und sonstigen Schäden durch Angriffe auf globale Informations- und Kommunikationssysteme entstehen können. Auf der anderen Seite sind diese Fälle aber auch Beleg dafür, dass nach wie vor eine vermeidbare Leichtfertigkeit im Umgang mit IT-Systemen weit verbreitet ist.

Präventive Maßnahmen sowie Anstrengungen zur Steigerung des Sicherheitsbewusstseins sind daher wesentliche Optionen zur Gefahrenminimierung.

Handlungsbedarf

allgemein

Wir müssen uns alle die Frage stellen: Sind die Entwickler und Betreiber von IT-Systemen, aber auch die Strafverfolgungsbehörden in Deutschland, angemessen

darauf eingestellt, Risiken und Schwierigkeiten beim Umgang mit IuK-Technik und IuK-Kriminalität frühzeitig zu erkennen und angemessen zu bewältigen.

Es gilt, neben den notwendigen Maßnahmen im nationalen Bereich zu Fragen der Organisation, der Aus- und Fortbildung, der Rechtsfortentwicklung und der Ausstattung mit ausreichenden und modernen Ressourcen vor allem die Zusammenarbeit im internationalen Bereich zu betrachten.

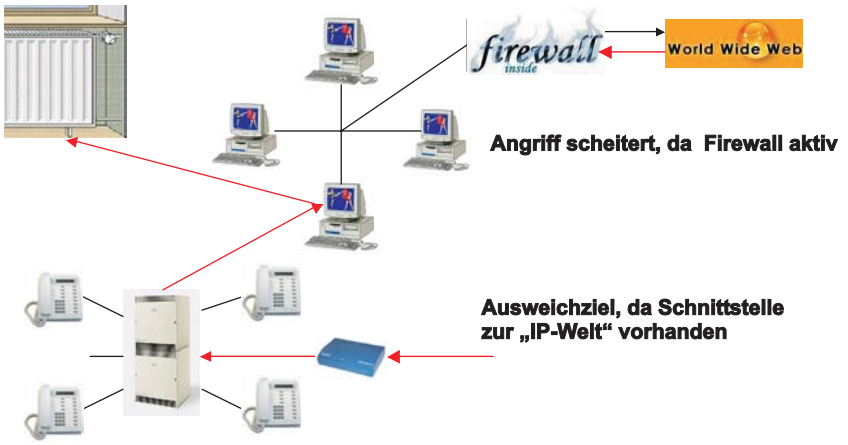
BKA-TeSIT

Das BKA hat sich bereits frühzeitig auf die neuen Entwicklungen im Bereich der IuK-Kriminalität eingestellt. Einerseits nimmt es als kriminalpolizeiliche Aufgabe die Phänomenzuständigkeit (Auswertung und Ermittlungen) wahr.

Daneben hat es zum Jahresbeginn 2002 das Technische Servicezentrum Informations- und Kommunikationstechnologien (TeSIT) eingerichtet.

In diesem Servicezentrum erfolgt nicht nur eine umfassende Analyse und Bewertung neuer Technologien hinsichtlich ihrer kriminogenen Faktoren und polizeilichen Nutzungsmöglichkeiten, sondern insbesondere auch eine intensive Forschung und Entwicklung, zum Beispiel im Bereich der Datenträgersicherung, -sichtung und -untersuchung.

„Lage, Bedrohungsszenarien und Handlungsbedarf“



Operativ liegt der Schwerpunkt in der Unterstützung polizeilicher Ermittlungen durch Sicherstellung und Analyse von Datenträgern bis hin zu Mobiltelefonen. Darüber hinaus findet im TeSIT die anlassunabhängige Recherche nach strafrechtlich relevanten Inhalten in Datennetzen statt. Schwerpunkte bilden Strafta-

ten der Kinderpornografie und des Rauschgifthandels, aber auch des illegalen Handels mit Arzneimitteln sowie der Hehlerei.

Aus- und Fortbildung von Polizei und Justiz

Die Anforderungen an Polizei und Staatsanwaltschaft zur kompetenten Bekämpfung der IuK-Kriminalität müssen aber schon in der Aus- und Fortbildung bei Polizei wie Justiz ansetzen.

Die Umsetzung vorliegender polizeilicher Konzepte zur angemessenen **Aus- und Fortbildung** im Bereich IuK werden wir weiter forcieren. Meine Aussagen zur Lage sowie zu realen wie potenziellen Bedrohungsszenarien machen deutlich, dass kurz- und mittelfristig weitere hohe Investitionen in die Bekämpfung der IuK-Kriminalität erforderlich sind.

Die Gewährleistung einer bundeseinheitlichen Aus- und Fortbildung verspricht eine ressourcenschonende aber gleichzeitig fachlich qualifizierte und aufeinander abgestimmte Aufgabenwahrnehmung im föderalen System.

Das Ausbildungskonzept sieht eine Staffelung von Fachkompetenz je nach Einsatzgebiet der Beamten vor. Ziel ist es, sowohl eine angemessene Anzeigenaufnahme als auch eine kompetente Sicherung von beweiserheblichen Daten in einer Computeranlage zu gewährleisten. Die Aus- und Fortbildungsmaßnahmen differenzieren zwischen dem polizeilichen Sachbearbeiter des „ersten Angriffs“ und den Sachbearbeitern für IuK-Kriminalität im weiteren und engeren Sinne. Zur letzten Gruppe gehört auch die IuK-Ermittlungsunterstützung sowie die forensische IuK. In dieser Gruppe wird der hohen Spezialisierung Rechnung getragen, das heißt, die Ausbildung vermittelt sowohl Kenntnisse zu diversen Betriebssystemen als auch zu Kryptographie und verschiedenen Speichermedien.

Internationale Zusammenarbeit

Internationale Ermittlungen zum Phänomen der IuK-Kriminalität erfordern in der Regel ein unverzügliches Handeln, da die Flüchtigkeit der beweiserheblichen Daten eine besondere Herausforderung in diesem Kriminalitätsbereich darstellt. Der Bedarf an einem schnellen und gut funktionierenden internationalen Informationsaustausch erfordert neue Wege der Kooperation.

Die G 8-Staaten haben sich daher verständigt, so genannte **High Tech Points of Contact** im Rahmen eines 24/7 Netzwerkes einzurichten. Mittlerweile sind in 35 Staaten zentrale Ansprechpartner rund um die Uhr verfügbar, um insbesondere bei schwerwiegenden Angriffen auf IT-Systeme und kritische Infrastrukturen zeitnah und kompetent reagieren zu können. Dadurch wird ein unmittelbarer Informationsaustausch zu temporär gespeicherten, flüchtigen Daten wie IP-Adressen oder Logfiles sichergestellt. Derzeit werden diese neuen Übermittlungswege im Rahmen von Testszenarien erprobt und weiterentwickelt.

Rechtsfragen und -fortentwicklung

Neben diesen Fragen der Informationserhebung und -übermittlung stellen sich natürlich auch zahlreiche rechtliche Probleme, die eine Fortentwicklung des Rechts zu bedenken geben.

Durch die tägliche Arbeit der IuK-Dienststellen in Bund und Ländern wird eine verstärkte Wahrnehmung der Messfühlerfunktion in Bezug auf notwendige Anpassungen im Straf- und Strafverfahrensrecht innerhalb Deutschlands möglich.

Es ist eine anspruchsvolle Aufgabe, die richtige Balance zwischen dem Schutz personenbezogener Daten, wirtschaftlichen Interessen und den Sicherheitsinteressen des Staates und der Bürger zu finden. Ich möchte beispielhaft die Problematik der Flüchtigkeit von Daten anführen. Die aktuelle Rechtslage lässt nur ein zeitlich begrenztes Vorrätighalten der Daten zu, soweit diese zum Zweck der Rechnungsstellung überhaupt erhoben worden sind. Bei so genannten flatrates und sonstigen anonymisierten Nutzungsmöglichkeiten, wie zum Beispiel Internetcafes, sind generell keine individualisierten Daten bei den Providern aufgezeichnet.

Die polizeiliche Praxis zeigt aber, dass Verdachtsmomente in Hinblick auf IuK-Straftaten erst mit zeitlicher Verzögerung bekannt oder ermittelt werden.

Der einzige Erfolg versprechende Ansatz zur Ermittlung der Verantwortlichen und zur Beweisführung sind die bei den Providern gespeicherten Daten. Wurden diese Daten überhaupt nicht erhoben oder sind sie bereits gelöscht, ist einer wirkungsvollen Strafverfolgung weitgehend der Boden entzogen. Ich möchte daher die Gelegenheit nutzen, aus Sicht einer Strafverfolgungsbehörde die Wichtigkeit der Einführung von angemessenen Mindestspeicherfristen zu betonen.

Mir ist sehr wohl bewusst, dass über eine weitergehende Erhebung und Speicherung von Daten für Zwecke der Strafverfolgung sowohl unter datenschutzrechtlichen Gesichtspunkten als auch unter Erwägungen der wirtschaftlichen Wettbewerbsfähigkeit zu diskutieren ist. Jedoch sollten empirische Daten der Strafverfolgungsorgane sowie Erfahrungen des Auslands mit weitergehenden Pflichten der Datenerhebung und -speicherung bei der nationalen Diskussion nicht zu kurz kommen.

Interdisziplinärer Ansatz

Alle Bemühungen der Strafverfolgungsorgane allein reichen jedoch nicht aus, den kriminogenen Faktoren der IuK-Technologien umfassend und ausreichend begegnen zu können.

Gemeinsam mit anderen gesellschaftlichen Kräften müssen wir für ein Umdenken im Umgang mit der letztendlich immer noch jungen Technik sorgen. Bei allen Nutzern muss ein Unrechtsbewusstsein auch bei einzelnen Nutzungsformen des

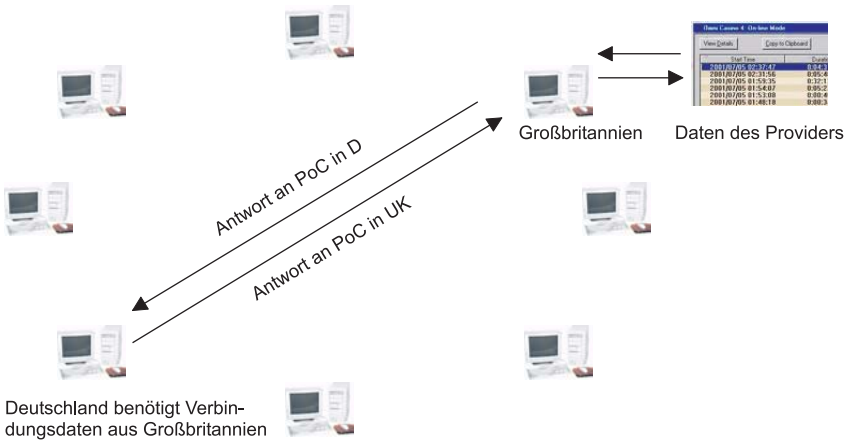
Internet, wie zum Beispiel beim illegalen Herunterladen von Software, Musik- und Filmtiteln geweckt werden. Nur weil dies technisch möglich ist und in einer vergleichsweise anonymen Umgebung stattfindet, heißt es noch lange nicht, dass es moralisch einwandfrei und rechtlich zulässig ist.

Das ist die eine Seite des Umdenkungsprozesses. Die andere ist die Veränderung des Sicherheitsdenkens. Wir müssen schon bei der Entwicklung wie beim Betreiben von IT-Systemen standardmäßig Schutzmechanismen vorsehen, um uns vor kriminellen Angriffen zu schützen. Firewalls und Virenschutzprogramme sollten auf jedem PC installiert sein und regelmäßig aktualisiert werden. Dazu sind verstärkte Zusammenarbeitsformen zwischen Industrie, Handel und Strafverfolgungsbehörden notwendig, um dem Aspekt der Datensicherheit einen höheren Stellenwert zu verschaffen.

Beispielhaft sei hier die Installation so genannter „honeypots“ genannt.

„Lage, Bedrohungsszenarien und Handlungsbedarf“

nationale Kontaktpunkte des G8 24/7-Netzwerks



Honeypots sind IT-Systeme, die potenziellen Angreifern als erreichbares Ziel angeboten werden, ohne dass die „echten“ IT-Systeme in Mitleidenschaft gezogen werden. Dadurch können sowohl Schäden abgewehrt als auch Angriffe und Angreifer erkannt werden. Zudem ermöglicht die Analyse von Angriffen auf „honeypots“ bessere Erkenntnisse über aktuelle Angriffsvarianten.

Auch die Trias Mensch-Technik-Organisation muss sich den ändernden Anforderungen und Rahmenbedingungen anpassen. Was nützt die beste Sicherheitstechnik, wenn das Passwort zu brisanten Daten auf einem gelben Klebezettel am Bildschirm befestigt ist?

public-private-partnership

Deshalb sollten im Rahmen von public-private-partnerships öffentliche und private Organisationen und Institutionen Lösungsstrategien entwickeln und anbieten und zum beiderseitigen Nutzen einen hohen Grad der Sicherheit für die Anwender von IuK-Technik gewährleisten. Gerade der Bereich der polizeilichen Präventionsarbeit sollte hier eine Pilotfunktion übernehmen.

Ausblick

Der britische Zukunftsforscher John C. Edwards sagte einmal: „Wenn es im Jahre 1879 schon Computer gegeben hätte, würden diese vorausgesagt haben, dass man infolge der Zunahme von Pferdewagen im Jahre 1979 im Pferdemist ersticken würde."

Das heißt im Ergebnis: Eine schlicht lineare Fortentwicklung bisheriger Trends alleine ist kein geeignetes prognostisches Instrument. Es steigen allerdings die Wahrscheinlichkeiten für kriminelle Aktivitäten im Zusammenhang mit der IuK. Die Strafverfolgungsorgane sind gut beraten, frühzeitig und antizipativ zu handeln.

Die IuK-Kriminalität wird künftig noch stärker als heute ein bedeutsames Tätigkeitsfeld für Polizei und Justiz sein. Laut ARD/ZDF-Online Studie 2003 nahm die Zahl der Internet-User im Vergleich zum Vorjahr um 22 % zu. Somit sind momentan 34,4 Mio. Personen über 14 Jahre in Deutschland online. Insbesondere die Neu-User stellen zu einem großen Teil potenzielle Opfer dar.

In Zeiten, in denen die Stärkung der Wirtschaft durch Entbürokratisierung und Liberalisierung erste Maxime politischen Handelns ist, bedarf es besonderer, aber auch besonnener Aktivitäten der Strafverfolgungsbehörden, um permanent auch auf die Risiken einer solchen Politik hinzuweisen.

Nicht die Verteufelung der IuK-Technologien ist angezeigt, sondern eine rationale und auf empirisch belegbaren Daten entwickelte Kriminalpolitik, die den Gefahrenpotenzialen der neuen Technologien angemessene Grenzen setzt.

Es geht um Grenzen, die ohne Gefährdung der wirtschaftlichen Notwendigkeiten dem Ziel einer effektiven, weltweiten Strafverfolgung Rechnung tragen. „Inseln der Straflosigkeit" können nicht hingenommen werden – im Ergebnis würden solche Zustände die Zukunft und das Vertrauen in die IuK-Technologie insgesamt schmälern und gefährden.

Insofern darf ich die Fragestellung meines Vorredners „Schöne neue Welt?" mit einem überzeugten „ja, aber" beantworten.

Weder blinder Fortschrittsglaube noch unreflektierte Forderungen nach Verschärfung staatlicher Eingriffsmaßnahmen helfen weiter. Vielmehr ist eine ganzheit-

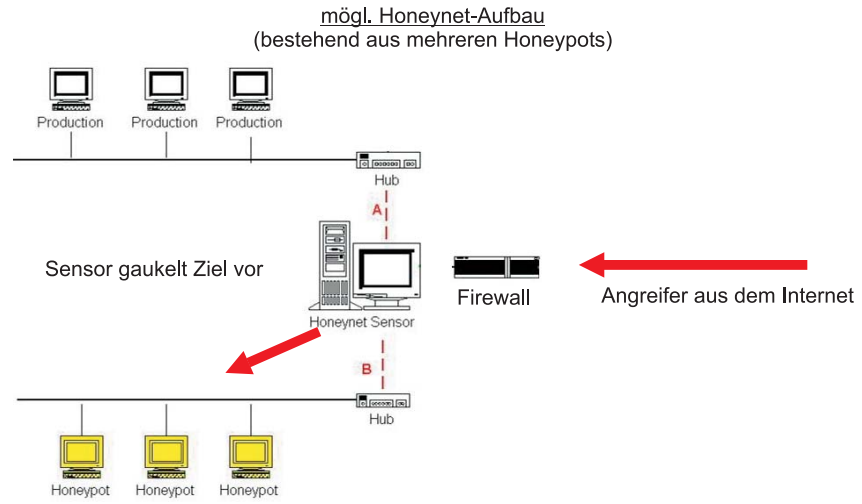
liche und ausgewogene Betrachtung von Chancen und Risiken oberste Maxime – auch für die Strafverfolgung.

– Den hier anwesenden Verantwortlichen für den Einsatz der Polizei möchte ich den Rat geben, sich organisatorisch, personell (Anzahl und Qualifikation der Mitarbeiter) sowie mit der Ausstattung (Hardware wie Software) den neuen Herausforderungen zu stellen, soweit dies noch nicht oder nicht ausreichend geschehen ist.
– Den IT-Entwicklern gilt der Wunsch, Belange der IT-Sicherheit bereits planerisch zu berücksichtigen.
– Die IT-Betreiber, Netzanbieter und Provider sollten – auch unter Kostengesichtspunkten – der IT-Sicherheit einen größeren Stellenwert einräumen. Im Falle eingetretener Angriffe oder Schäden sollten sie offensiv die Polizei einschalten.

Nur gemeinsam können wir uns des Problems ernsthaft annehmen; diese Veranstaltung ist ein wichtiger Schritt in diese Richtung.

Ich danke für Ihre Aufmerksamkeit.

„Lage, Bedrohungsszenarien und Handlungsbedarf“



Zur Zusammenarbeit der Strafverfolgung mit Service-Providern

Ralf Günther

1 Einleitung

Herr Präsident, meine Damen und Herren, ich möchte mich zunächst für die Gelegenheit bedanken, im Rahmen einer Veranstaltung wie dieser einige Gedanken aus staatsanwaltschaftlicher Sicht zur Zusammenarbeit der Strafverfolgungsbehörden mit den Service-Providern darlegen zu dürfen. Da diese Gedanken vorwiegend auf den Erfahrungen basieren, die ich als Dezernent der Zentralen Stelle Organisierte Kriminalität und Korruption (ZOK) der Generalstaatsanwaltschaft Celle gewonnen habe, gestatten sie mir, auch zum besseren Verständnis des Nachfolgenden, kurz einige der Funktionen der ZOK zu erläutern.

Niedersachsen hat die ZOK im Jahre 1996 eingerichtet. Die ZOK ist Teil der Generalstaatsanwaltschaft Celle, aber landesweit zuständig, also auch für die Bezirke der Generalstaatsanwaltschaften Braunschweig und Oldenburg. Zur Kernaufgabe der ZOK gehört die Beratung und Information aller mit Organisierter Kriminalität, Korruption, Gewinnabschöpfung, Geldwäsche und Internationaler Zusammenarbeit befassten Dienststellen von Polizei und Staatsanwaltschaft. Trotz insoweit bestehender gesetzlicher Regelungen entstehen immer wieder Fragen zu rechtlichen Problemen, etwa zur Zulässigkeit verdeckter Ermittlungsmaßnahmen, Fragen zur Korruption oder der Gewinnabschöpfung. Hierzu entwickelt die ZOK Lösungen, die innerhalb Niedersachsens und gegebenenfalls auch bundesweit abgestimmt werden. Dies gibt den Strafverfolgungsbehörden ein hohes Maß an Rechtssicherheit.

Gleiches gilt auch für den Bereich der Telekommunikationsüberwachung.

Die ZOK erhält darüber hinaus entsprechende Informationen sowie Erfahrungsberichte, auch über die Zusammenarbeit mit den Service-Providern, durch die Generalstaatsanwaltschaften der anderen Bundesländer. Diese Unterrichtung basiert auf einer Vereinbarung der OK-Koordinatoren sämtlicher Generalstaatsanwaltschaften, wonach die ZOK für den Bereich der Telekommunikationsüberwachung innerhalb dieses Gremiums eine gewisse Sprecherfunktion wahrnimmt.

Bei der Klärung sämtlicher so an die ZOK herangetragenen Rechtsfragen mit grundsätzlicher Bedeutung nimmt diese regelmäßig auch Kontakt mit den betroffenen Netzbetreibern, den Service-Providern beziehungsweise der Regulierungsbehörde für Telekommunikation und Post (RegTP) auf. Die ZOK steht somit in einem engen und aus meiner Sicht auch vertrauensvollen Meinungsaustausch mit diesen Stellen.

Um schließlich über die in des Wortes bestem Sinne augenblickliche Praxis der Zusammenarbeit mit den Service-Providern unterrichtet zu sein, hat die ZOK

mit Schreiben vom 22. 9. 2003 sämtliche niedersächsischen Polizeibehörden, die niedersächsischen Staatsanwaltschaften, Dienststellen des Zolls und des Bundesgrenzschutzes sowie einzelne Generalstaatsanwaltschaften in anderen Bundesländern um entsprechende Stellungnahmen ersucht.

Auf alldem basieren die nachfolgenden Erwägungen.

Über rechtliche Probleme der Strafverfolgung berichtete OStA Ralf Günther

2 Rahmenbedingungen der Zusammenarbeit

Die Notwendigkeit der Zusammenarbeit von Service-Providern und Strafverfolgungsbehörden hat sich mit der Privatisierung der Telekommunikation im Zuge der Postreformen ergeben. Mit dieser Privatisierung wurden auch die technischen Einrichtungen für die Überwachung der Telekommunikation in eine privatrechtliche Sach- und Funktionsherrschaft überführt.

Der Gesetzes- und Verordnungsgeber hat hierfür unter anderem im Telekommunikationsgesetz (TKG), der Telekommunikations-Überwachungsverordnung (TKÜV) sowie in der Strafprozessordnung (StPO) die Rahmenbedingungen geschaffen und dabei zwei Gruppen mit völlig unterschiedlichen Interessenslagen beziehungsweise Aufgaben zu einer „Zwangsgemeinschaft“ mit primär wider-

streitenden Mitgliederinteressen verbunden. Es handelt sich dabei, gestatten Sie mir die saloppe Bemerkung, um keine wirkliche Liebesbeziehung.

Was die unterschiedlichen Interessenlagen anbelangt, so ist für die Diensteanbieter die Erwirtschaftung von Gewinnen, für die Strafverfolgungsbehörden eine geordnete und effiziente Strafverfolgung das zentrale Anliegen. Wirtschaftliche Erwägungen sind für letztere, jedenfalls noch, von untergeordneter Bedeutung.

Wie vorhersehbar führten allein schon die hieraus abzuleitenden unterschiedlichen Handlungsmaximen der Mitglieder dieser Gemeinschaft zu Schwierigkeiten in der Zusammenarbeit.

So wurde einerseits durch die Netzbetreiber die Regelung in § 88 Abs. 1 TKG kritisiert. Diese verpflichtet sie, die Überwachungstechnik auf eigene Kosten vorzuhalten. Hier erfolge, so die Kritik, eine Indienstnahme, ohne dass gesicherte Erkenntnisse über die Effektivität der Telekommunikationsüberwachung vorlägen. Auch die Durchführung von Überwachungsmaßnahmen sei nicht kostendeckend. Die Kostendeckung liege bei einzelnen Netzbetreibern lediglich im Bereich zwischen 1 % und 10 %. Dementsprechend ist von weiten Teilen der Literatur aber auch von Datenschutzbeauftragten eine Evaluierung gefordert worden.

Andererseits war bereits im Gesetzgebungsverfahren durch den Bundesrat die Sorge geäußert worden, die Betreiber könnten aus Wettbewerbsgründen eine Zusammenarbeit verweigern (vgl. BR-Drs. 13/4438, S. 23).

3 Bedeutung der Telekommunikationsüberwachung

Die Strafverfolgungsbehörden haben seit jeher und einhellig die Auffassung vertreten, dass die Überwachung der Telekommunikation von herausragender, ja geradezu fundamentaler Bedeutung für eine effektive Strafverfolgung im Bereich der schweren und Organisierten Kriminalität ist. Entsprechend der Bedeutung dieses Ermittlungsinstruments ist die bundesweite Anzahl der TKÜ-Maßnahmen in den vergangenen Jahren kontinuierlich angestiegen – und damit auch die Indienstnahme der Service-Provider.

Eine der maßgeblichen Ursachen für den Anstieg der TKÜ-Maßnahmen ist darin zu sehen, dass die Zahl der Mobilfunkanschlüsse von rund 3.800.000 im Jahre 1997 auf 56.200.000 im Jahre 2000 zugenommen hat.

Schließlich ist der Anstieg gerade auch dadurch bedingt, dass die Beschuldigten und sonstigen Betroffenen häufig ihre Telefonkarten wechseln und in Deutschland eine IMEI-bezogene Telekommunikationsüberwachung technisch noch nicht durchgängig möglich und rechtlich umstritten, nach richtiger Auffassung aber zulässig ist.

Auch der Anstieg der TKÜ-Maßnahmen ist von den Medien, den Datenschutzbeauftragten und nicht zuletzt auch von den Vertretern der Service-Provider stets

kritisch bewertet worden. Um so erfreulicher ist, dass mit der Studie des Max-Planck-Institutes für Ausländisches und Internationales Strafrecht zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, b StPO und anderer verdeckter Ermittlungsmaßnahmen" nunmehr erstmals eine umfassende Evaluierung vorliegt. Diese ist, neben auch kritischen Erwägungen, in ihrer abschließenden Bewertung unter anderem zu folgendem Ergebnis gelangt – ich zitiere: „Die TKÜ ist als ein wichtiges und unabdingbares Ermittlungsinstrument einzuschätzen, das in bestimmten Bereichen nachvollziehbare und grundlegende Erfolge erzielt. Dies gilt vor allem für den Bereich der Transaktionskriminalität, der als opferlose Kriminalität eines proaktiven Ansatzes in den Ermittlungen bedarf, soll Strafrecht überhaupt implementiert werden."

4 Aspekte der Zusammenarbeit

Die Zusammenarbeit zwischen den Service-Providern und den Strafverfolgungsbehörden ist eine unter praktischen, technischen und, worauf sich meine Ausführungen konzentrieren werden, rechtlichen Gesichtspunkten ausgesprochen komplexe Problematik, die in der mir zur Verfügung stehenden Zeit nur punktuell beleuchtet werden kann.

Die Zusammenarbeit kann, trotz nach wie vor bestehender Defizite und der pauschalen Bewertungen stets immanenten Ungenauigkeit in jüngerer Zeit als weitgehend zufriedenstellend bezeichnet werden.

Dass sie nicht noch besser ist, dürfte, neben Defiziten auf Seiten der Strafverfolgungsbehörden, auch an den Service-Providern selbst liegen. Ich darf insoweit beispielhaft auf aktuelle, wenngleich zwischenzeitlich wieder beseitigte Kapazitätsengpässe bei Netzbetreibern verweisen, die bei einer vorausschauenderen Planung vermutlich vermeidbar gewesen wären. Weiterhin sind die bestehenden Defizite aber auch darin begründet, dass die Länder, worauf bereits im Gesetzentwurf des Bundesrates vom 31. Mai 2002 (BR-Drs. 275/02, S. 16) hingewiesen worden war, beim Erlass und bei Änderungen der für die Praxis so wichtigen TKÜV nur unzureichend beteiligt waren. Dabei sind sie es, die in erster Linie mit der Durchführung der Strafverfolgung betraut sind. Deswegen dürften Defizite im Bereich der Telekommunikationsüberwachung auch zuerst auf Länderebene sichtbar werden.

Schließlich dürfte ein beachtlicher Anteil der bestehenden Defizite in der Zusammenarbeit zwischen Service-Providern und Strafverfolgungsbehörden, dies mag überraschen, in der bestehenden, teilweise nicht eindeutigen und insgesamt nicht ausreichend harmonisierten Gesetzes- und Verordnungslage begründet sein und damit im Verantwortungsbereich des Normgebers liegen. Dabei ist bezüglich dieses „Normgebers" anzumerken, dass für die Änderungen der gesetzlichen „Rahmenbedingungen" unterschiedliche Zuständigkeiten bestehen. So ist bei Novel-

lierungen der StPO das Bundesjustizministerium, bei Novellierungen von TKG und TKÜV das Bundesministerium für Wirtschaft und Arbeit federführend. Näheres zu alledem später.

5 Aktuelle Rechtslage, Fragestellungen im Zusammenhang mit den §§ 100 a, b, g und h StPO

Doch wie, meine Damen und Herren, sieht die aktuelle Rechtslage im Bereich der Telekommunikationsüberwachung bezüglich der zentralen Eingriffsermächtigungen, der §§ 100 a, b, 100 g, h StPO aus? Sie sind es, die zusammen mit den Vorschriften des TKG sowie der TKÜV die gesetzlichen Rahmenbedingungen für die Praxis der Zusammenarbeit mit den Service-Providern bilden.

Mögliche Lücken, Unklarheiten und Widersprüche innerhalb einer dieser Normen beziehungsweise in ihrem Verhältnis zueinander wirken sich unmittelbar auch auf die Zusammenarbeit aus. Dies gilt vorrangig dann, wenn die Service-Provider bei ihrem Normverständnis im Einzelfall die Eingriffsvoraussetzungen als nicht gegeben ansehen und deshalb ihre geforderte Mitwirkung versagen. Daher bedarf es bezüglich der jeweiligen Eingriffsvoraussetzungen der Normenklarheit.

Was diese und damit die aktuelle Rechtslage anbelangt, möchte ich Ihnen beispielhaft nur einige wenige der von Polizeibehörden und Staatsanwaltschaften in der Vergangenheit an die ZOK herangetragene Probleme beziehungsweise Fragestellungen bezüglich der §§ 100 a, b StPO beziehungsweise der TKÜV anführen:

- Rechtliche Möglichkeit einer gerätenummerbezogenen (IMEI-) Überwachung von Mobiltelefonen (vgl. vorstehend 3).
- Vormalige Praxis einzelner Netzbetreiber, die Geo-Daten bei Stand-by-Funktion des Handys entgegen der Regelung in § 7 Abs. 1 Nr. 7 TKÜV nicht zu übermitteln.
- Rechtsgrundlage für die Erhebung der auf einem E-Mail-Server zwischengespeicherten Daten.
- Rechtmäßigkeit der Praxis einzelner Netzbetreiber, für den im Zusammenhang mit Überwachungsanordnungen erforderlichen Informationsaustausch ausschließlich die besonders gebührenträchtigen 0190er Nummern zur Verfügung zu stellen.
- Inhaltliche Anforderungen an eine Anordnung gemäß § 100 b Abs. 2 S. 2 StPO; muss diese stets Namen und Anschrift des Betroffenen enthalten?
- Adressatenkreis der durch § 100 b Abs. 1 StPO verpflichteten Netzbetreiber beim so genannten Roaming-Verfahren. Sind einzelne Netzbetreiber ver-

pflichtet, die ihnen übermittelten Anordnungen ihren Roaming-Partnern vorzulegen?

- Fristberechnung bei § 100 b StPO in Fällen so genannter „Kettenbeschlüsse", in denen auf die Erstanordnung bezüglich eines bestimmten Anschlusses bereits zu einem Zeitpunkt Verlängerungsanordnungen ergehen, zu dem die für die Erstanordnung geltende Frist noch nicht abgelaufen ist.
- Form und Inhalt einer Überwachungsanordnung bei besonderer Dringlichkeit ihrer Umsetzung gemäß § 12 Abs. 2 TKÜV.

Bezogen auf die §§ 100 g, h StPO sind unter anderem folgende Fragestellungen an die ZOK herangetragen worden:

- Auslegung des Merkmals „Straftat von erheblicher Bedeutung" in § 100 g Abs. 1 Satz 1 StPO und seine Abgrenzung von den Katalogtaten in § 100 a Satz 1 StPO.
- Verhältnis von staatsanwaltschaftlicher Eilanordnung auf Auskunftserteilung gemäß § 100 g Abs. 1 Satz 3 StPO und der Löschungsverpflichtung nach der TDSV, wenn die richterliche Bestätigung nicht binnen drei Tagen eingeht.
- Bedarf die auf der Grundlage einer staatsanwaltschaftlichen Eilanordnung gemäß § 100 h Abs. 1 Satz 2 StPO erfolgte Übermittlung ausschließlich retrograder Verbindungsdaten der richterlichen Bestätigung gemäß §§ 100 h Abs. 1 Satz 3, 100 b Abs. 1 StPO?
- Voraussetzungen für eine online- beziehungsweise digitale Übermittlung beziehungsweise Weitergabe von Verbindungsdaten gemäß § 100 g StPO durch die Provider an die Verpflichteten.
- Einschlägige Rechtsgrundlage für die Erhebung und Verwertung der in einem Mobiltelefon gespeicherten Daten wie Telefonverzeichnisse, Anruflisten, Kurznachrichten (so genannte SMS) unter anderem, Rechtsgrundlage für die Erhebung der PUK.

Die Praxis der Telekommunikationsüberwachung und damit der Zusammenarbeit ist mithin schon aus Rechtsgründen in erheblichem Maße, dies dürfte deutlich geworden sein, problembeladen. Bestehende gesetzliche Regelungen bedürfen einer Klarstellung. So ist beispielsweise § 100 g Abs. 1 StPO, der der Praxis in der Anwendung erhebliche Schwierigkeiten bereitet, von einer Strafkammer als grammatikalisch unvollständig bezeichnet worden (LG Wuppertal, MMR 2002, 560).

6 Ausgewählte Einzelfälle

Gestatten Sie mir, Ihnen die Problematik an zwei der bereits angesprochenen Fälle, der IMEI-Problematik sowie der Erhebung retrograder Verbindungsdaten gemäß §§ 100 g, h StPO, vertiefend zu erläutern.

Nach richtiger Auffassung, so auch der Ermittlungsrichter beim BGH in seinen Beschluss vom 7. 9. 1998, ist sie zulässig. Die meisten Netzbetreiber hingegen stützen ihre ablehnende Auffassung auf § 2 Nr. 6 TKÜV, wonach „Kennung" das auf eine Person bezogenen technische Merkmal zur Überwachung der Telekommunikation ist.

Die ZOK hatte diese Problematik bereits Anfang 1998 aufgegriffen und sich sowohl an die Netzbetreiber als auch an die Regulierungsbehörde für Telekommunikation und Post (RegTP) gewandt. Diese hat zu der Problematik vornehmlich in rechtlicher Hinsicht Stellung bezogen. Sie hat gleichzeitig aber auch darauf hingewiesen, dass sich ihr unmittelbarer Zuständigkeitsbereich insoweit auf die Genehmigung und die Abnahme technischer Einrichtungen beschränke. Die RegTP vermochte die Frage, ob einzelnen Netzbetreibern eine IMEI-bezogene Überwachung möglich ist, mithin nicht zu beantworten. Die ZOK hat in der Folgezeit über Jahre versucht, zuverlässig festzustellen, ob die Netz- und Softwarekonfigurationen der Betreiber eine solche Maßnahme zulassen beziehungsweise mit welchem Aufwand eine Nachrüstung verbunden wäre.

Die Frage hat, ungeachtet der Initiative des Bundesrates vom 31. 5. 2002 (vgl. BR-Drs. 275/02), wonach die einschlägige Regelung der TKÜV dahingehend ergänzt werden sollte, dass auch ausschließlich hardwarebezogene Merkmale eine Kennung im Sinne dieser Verordnung darstellen sollen, mit der Einführung des § 100 i StPO durch das Gesetz zur Änderung der Strafprozessordnung vom 6. 8. 2002 eine neue Aktualität erfahren. Der Gesetzgeber hat in § 100 i Abs. 1 Nr. 1 StPO ausdrücklich festgelegt, dass zur Vorbereitung einer Maßnahme nach § 100 a StPO die Geräte- und Kartennummer ermittelt werden kann. Diese Regelung kann nur so verstanden werden, dass im Gegensatz zum Verordnungsgeber der TKÜV der Bundesgesetzgeber offensichtlich von der Zulässigkeit auch einer gerätebezogenen Telekommunikationsüberwachung ausgegangen ist. Nur in diesem Fall macht es überhaupt Sinn, wie hier geregelt, „zur Vorbereitung einer Maßnahme nach § 100 a StPO die Gerätenummer . . ." zu ermitteln.

Dieses Beispiel macht deutlich, wie schwierig und auch langwierig die Lösung telekommunikationsrechtlicher Fragen sein kann – wobei hier eine Lösung noch immer nicht erreicht werden konnte.

Obwohl diese für die Praxis wichtige Problematik damit seit Jahren bekannt ist, findet die Rechtsauffassung des BGH auch im aktuellen Entwurf zur Änderung der TKÜV noch keine Berücksichtigung.

Zu ganz erheblichen Schwierigkeiten für die Praxis im vergangenen Jahr führte auch die Handhabung eines Netzbetreibers, Eilanordnungen der Staatsanwaltschaft gemäß §§ 100 h Abs. 1 S. 3, 100 b Abs. 1 S. 2 und 3 StPO auf Übermittlung von Verbindungsdaten bis zur Vorlage einer richterlichen Bestätigung nicht nachzukommen.

Regelmäßig wurde dabei angekündigt, die Daten zu löschen, falls die Bestätigung nicht binnen drei Tagen eingehe. Diese Vorgehensweise ist rechtswidrig.

Gegenvorstellungen haben keine aufschiebende Wirkung. Darüber hinaus dürfte vorliegend eine richterliche Bestätigung bei der Erhebung allein retrograder Daten nicht erforderlich sein. § 100 b Abs. 1 S. 3 StPO kann, da sich dieser auf die Aufzeichnung und Überwachung künftiger Telekommunikation bezieht, hier nur sinngemäß Anwendung finden. Da retrograde Daten in ihrem Gesamtbestand zum Zeitpunkt der Anordnung bereits vorhanden sind, dürfte die Eilanordnungskompetenz der Staatsanwaltschaft aufgrund der insoweit eindeutigen Verweisung in § 100 h StPO auch den Gesamtbestand dieser Daten erfassen.

Eine richterliche Bestätigung ist damit entbehrlich. Sinn und Zweck der richterlichen Bestätigung ist nicht, die Richtigkeit der staatsanwaltschaftlichen Eilanordnung zu überprüfen. Diese nimmt in Fällen der vorliegenden Art vielmehr mit der Ausübung ihrer Eilkompetenz eine ihr übertragene Befugnis in eigener Zuständigkeit wahr. Gegenstand der richterlichen Entscheidung ist vielmehr allein die Frage, ob die Voraussetzungen des § 100 a StPO zum Zeitpunkt der richterlichen Entscheidung noch immer vorliegen und ob die Maßnahme fortdauern soll (vgl. Nack in KK, StPO 5. Aufl., § 100 b Rdnr. 1, § 98 Rdnr. 21).

7 Umfrage

Nunmehr möchte ich ihnen die Ergebnisse der bereits angesprochene Umfrage darlegen. Sie sind nicht repräsentativ, bestätigen jedoch, dies darf ich vorwegnehmen, die insoweit vorliegenden übrigen Erkenntnisse der ZOK.

Durch die befragten Generalstaatsanwaltschaften wird die Zusammenarbeit zwischen der Strafverfolgung und den Service-Providern gegenwärtig als zufriedenstellend bezeichnet. Probleme werden hier allein insoweit beschrieben, als es unterschiedliche Auffassungen zu der Frage gebe, auf welcher Rechtsgrundlage die „hinter" dynamischen IP-Adressen bestehenden Personen identifiziert, das heißt deren Personendaten erhoben werden können. Während dort § 89 Abs. 6 TKG als einschlägig angesehen werde, würden Provider die Auffassung vertreten, entsprechende Daten könnten allein auf der Grundlage der §§ 100 g, h StPO erhoben werden.

Die in den Berichten der Staatsanwaltschaften enthaltenen Aspekte über die Zusammenarbeit zwischen der Strafverfolgung und den Service-Providern, in 25 % der Fälle wurde hier Fehlanzeige erstattet, beziehen sich ausschließlich auf den Bereich der Sprachtelefonie.

Insoweit ergibt sich folgende Verteilung:

- Probleme bei der Verbindungsdatenerhebung gemäß §§ 100 g, h StPO: 50 %
- Probleme im Zusammenhang mit § 12 TKÜV: 33 %
- Schwierigkeiten bei der Rechnungslegung durch die Service-Provider: 17 %

Die Berichte der niedersächsischen Polizeibehörden, des Zollfahndungsamtes Hannover sowie der angeschriebenen Dienststellen des Bundesgrenzschutzes sind ausgesprochen detailliert. Alle berichtenden Behörden legen Probleme dar, enthalten mithin keine Fehlanzeige.

Von den beschriebenen Problemen beziehen sich 96 % auf den Bereich der Sprachtelefonie und 4 % auf den der Internetüberwachung. Hinsichtlich des Problembereichs Sprachtelefonie ergibt sich folgende Verteilung:

- Erhebung von Bestands-/Kundendaten gemäß §§ 89 Abs. 6, 90 TKG: 46 %
- Erhebung von Verbindungsdaten gemäß §§ 100 g, h StPO: 23 %
- Erhebung von Inhaltsdaten gemäß §§ 100 a, b StPO: 22 %
- Probleme im Zusammenhang mit der Rechnungslegung: 9 %

Innerhalb des Problembereichs der §§ 89 Abs. 6, 90 TKG ist folgende Gewichtung festzustellen:

- Unvollständige beziehungsweise unzutreffende Auskünfte im automatisierten Abrufverfahren nach 90 TKG: 45 %
- Fehlende beziehungsweise falsche Datenerhebung bei Prepaid-Karten: 36 %
- Sonstige Probleme (Erhebung von Bestandsdaten bei Rufnummer-Portierung und anderes): 19 %

Im Zusammenhang mit der Erhebung von Verbindungsdaten gemäß §§ 100 g, h StPO ergibt sich folgende Verteilung:

- Übermittlung von Verbindungsdaten zu langsam: 55 %
- Probleme im Zusammenhang mit dem Zielsuchlauf: 18 %
- Probleme bei der Erhebung der PUK, Weigerung der Diensteanbieter diese ohne Beschluss gemäß §§ 100 g, h StPO herauszugeben: 5 %
- Sonstige Probleme: 22 %

Hinsichtlich der Erhebung von Inhaltsdaten stellt sich die Problemverteilung wie folgt dar:

- Fehlende Möglichkeit einer IMEI-bezogenen Telekommunikationsüberwachung: 38 %

- Formale Beanstandungen durch die Netzbetreiber/Service-Provider: 22 %
- Fehlende Möglichkeiten bei der Erhebung von Auslandsdaten: 15 %
- Sonstige Probleme: 25 %

Interessant erscheint, dass die meisten Probleme offensichtlich nicht mit der Erhebung der besonders eingriffsintensiven Inhaltsdaten, sondern mit der Erhebung der Bestands-, Kunden- und Verbindungsdaten verbunden sind.

8 Verordnungs- und Gesetzesnovellierungen

Die Zusammenarbeit der Strafverfolgungsbehörden mit den Service-Providern wird auch dadurch geprägt, dass die gesetzlichen Rahmenbedingungen für die hier allein zu betrachtende „Individualkontrolle" ständigen Novellierungen unterworfen sind. Die Ursachen hierfür liegen unter anderem in der rasanten technischen Entwicklung von Informations- und Kommunikationstechnik.

Erwähnt seien insoweit nur Stichworte wie „Digitalisierung der Telekommunikation" und „Multimediadienste", Entwicklungen denen sich auch die Rechtsordnung anpassen muss. Sie liegen aber auch in der Tatsache begründet, dass die Mitglieder der „Zwangsgemeinschaft" ständig versuchen, die gesetzlichen Rahmenbedingungen jeweils ihrer Interessenlage anpassen zu lassen.

Auf die damit einhergehenden rechtlichen Konsequenzen, insbesondere bei einer tatsächlich oder zumindest nach der jeweils eigenen Auffassung nicht eindeutigen Rechtslage, mussten und müssen sich beide Parteien erst einstellen – nicht selten unter Anrufung der Beschwerdegerichte durch die Provider.

Als Beispiele für erfolgte Novellierungen seien das Gesetz zur Änderung der StPO vom 20. 12. 2001, durch das die §§ 100 g, h StPO als Nachfolgeregelung des § 12 Fernmeldeanlagengesetz (FAG) in die StPO eingefügt worden war, die TKÜV vom 22. 1. 2002 und die Erste Verordnung zur Änderung der TKÜV vom 12. 6. 2002 erwähnt. So sah § 12 Abs. 2 TKÜV zunächst eine Frist von nur drei Tagen für die Übersendung der Überwachungsanordnung vor und stellte die Praxis damit vor erhebliche, unnötige Schwierigkeiten, bevor die Frist durch die Erste Verordnung zur Änderung der TKÜV auf eine Woche verlängert worden ist.

Gerade die Auslegung der §§ 100 g, h StPO beziehungsweise die Anwendung des § 12 TKÜV führten zu erheblichen Differenzen.

Weitere Änderungen, unter anderem in der TKÜV sowie dem TKG, und damit verbunden weitere mögliche Differenzen bei deren Auslegung werden folgen. So ist unter anderem beabsichtigt, im Interesse der Strafverfolgungsbehörden § 12 Abs. 2 TKÜV innerhalb von voraussichtlich weniger als neun Monaten erneut zu überarbeiten und festzuschreiben, dass unter bestimmten Voraussetzungen auf die Vorlage des Originals beziehungsweise einer beglaubigten Abschrift

der Überwachungsanordnung verzichtet werden kann. Auch die für die Praxis der Strafverfolgungsbehörden wichtigen Regelungen der §§ 89 und 90 TKG sollen in den §§ 110, 111 TKG-Entwurf (Stand: Regierungsentwurf) neu gefasst werden.

Die §§ 89, 90 TKG enthalten unter anderem die Rechtsgrundlage für die Erhebung der so genannten Bestands- und Kundendaten.

So sieht § 110 Abs. 1 Satz 3 TKG-Entwurf vor, dass in Fällen der Rufnummer-Portabilität Rufnummer und Portierungskennung erst ein Jahr nach dem Zeitpunkt zu löschen sind, zu dem die Rufnummer an den Netzbetreiber zurückgegeben wurde. Diese Regelung dient damit dem Interesse der Strafverfolgungsbehörden.

§ 111 Abs. 2 Satz 2 TKGE regelt eine bisherige Streitfrage und legt fest, dass den Telekommunikationsunternehmen für die Erteilung von Auskünften eine Entschädigung wie nach § 17 a ZSEG gewährt wird. Darüber hinaus stellt Satz 3 des Entwurfs nunmehr klar, dass hier eine Entschädigung auch zu zahlen ist, wenn sich das Auskunftsbegehren lediglich auf solche Daten bezieht, die auch im automatisierten Verfahren nach § 110 TKG-Entwurf (§ 90 Abs. 4 TKG) abrufbar wären. Diese Regelung dient dem Interesse der Provider.

9 Argumentation „pro domo“

Die in der Praxis der Zusammenarbeit regelmäßig zu Schwierigkeiten führende unterschiedliche Auslegung nicht eindeutiger Gesetze und Verordnungen dürfte – sprechen wir es offen aus – nicht unerheblich auch dadurch beeinflusst werden, welcher „Seite“ man angehört, den Service-Providern oder den Strafverfolgungsbehörden.

Es ist mir ein besonderes Anliegen, gerade diesen Gesichtspunkt anzusprechen, weil nur eine offene, auch die spezifischen Interessen der anderen Seite berücksichtigende Meinungsbildung und auf ihr basierend eine ausgewogene Diskussion eine sachgerechte Interessenabwägung und Normsetzung ermöglicht.

Wichtig ist auch, bestehende Fehlvorstellungen, Missverständnisse etc. zu erkennen und zu beseitigen.

So ist auf verschiedenen Tagungen mit Vertretern der Service-Provider deutlich geworden, dass einige der Teilnehmer davon ausgegangen sind, staatsanwaltschaftliche Eilanordnungen seien zu einem beachtlichen Teil rechtswidrig. Aus ihnen vorliegenden Statistiken ergebe sich, dass diese nicht richterlich bestätigt worden seien. Unbekannt war, dass die so gewonnenen Erkenntnisse auch ohne richterliche Bestätigung verwertbar sind und dass es ihrer stets dann nicht bedarf, wenn die Maßnahme, was nicht selten vorkommt, nicht länger als drei Tage dauern soll.

10 Systematik der Eingriffsnormen

Nicht nur zur Beseitigung bestehender und Vermeidung künftiger Probleme und damit auch zur Gewährleistung einer effizienten Zusammenarbeit zwischen Service-Providern und Strafverfolgungsbehörden, sondern auch aus weiteren, grundsätzlichen Erwägungen, etwa zur Wahrung der verfassungsmäßigen Rechte Betroffener, sind die Strafverfolgungsbehörden auf ein rechtliches Instrumentarium der Telekommunikationsüberwachung angewiesen, welches nicht nur die Eingriffsvoraussetzungen klar umschreibt, sondern auch – in einem stärkeren Maße als bisher – die Vorschriften von StPO, TKG und TKÜV zu einem harmonischen Ganzen fügt.

Was die „Gemeinschaft" von Service-Providern und Strafverfolgungsbehörden hinsichtlich der bereits jetzt sicher absehbaren Novellierungen, etwa der der §§ 100 g, h StPO, künftig erwartet, vermag heute noch niemand sicher abzusehen.

Doch auch bzgl. der aktuellen Rechtslage erscheint mir der Versuch lohnend, eine Harmonie im Verhältnis der §§ 100 a, b, §§ 100 g, h und § 100 i StPO zu suchen.

Gestatten Sie mir deshalb, Ihnen schlagwortartig folgenden Aufriss zu einem möglich erscheinenden Verhältnis der §§ 100 a, b, §§ 100 g, h, § 100 i StPO sowie der §§ 89, 90 TKG darzulegen.

1. Das Fernmeldegeheimnis des Art. 10 GG schützt die durch die Diensteanbieter vermittelte Telekommunikation und erfasst neben dem Inhalt der individuellen Nachrichtenübermittlung auch deren näheren Umstände. Zu diesen gehört insbesondere, „ob, wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist" (vgl. BVerfG, Urteil vom 14. 7. 1999, NJW 2000, S. 55, 56, mit Verweis auf BVerfGE 67, 157, 172). Zwar hat das BVerfG zutreffend gerade in seinen neueren Entscheidungen (vgl. BVerfG, Urteile vom 12. 3. 2003, NStZ 2003, S. 441, 442, sowie vom 14. 7. 1999, a. a. O.) hervorgehoben, die Nutzung von Telekommunikationsanlagen solle unbefangen möglich sein und nicht deswegen unterbleiben, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten. Deutlich hat das BVerfG indes auch hier festgestellt, dass vom Schutzbereich des Art. 10 GG (nur) die Kommunikationsinhalte und deren näheren Umstände geschützt werden. Die technische Eignung eines Gerätes, als Kommunikationsmittel zu dienen sowie die von diesem ausgehenden technischen Signale zur Gewährleistung dieser Bereitschaft dürften hingegen von Art. 10 GG nicht erfasst werden (so bzgl. der Bewegungsdaten Kudlich, JuS 2001, S. 1165, 1168; Bernsmann/Jansen, StV 1999, S. 591, 592). Erst die tatsächliche Nutzung zur menschlichen Kommunikation qualifiziert diese technischen Daten zu „Kommunikationsumständen" und damit zu Daten, die vom Schutzbereich des Art. 10 GG erfasst werden. Diese Auslegung

erscheint geboten, um den erforderlichen personalen Bezug der Grundrechte zu gewährleisten.

2. Eingriffe in das Fernmeldegeheimnis dürfen nur aufgrund eines Gesetzes angeordnet werden.

3. Derartige Eingriffe gestatten die §§ 100 a, b, 100 g, h StPO. Folgerichtig verpflichten diese, entsprechend dem vorstehend unter 1. aufgezeigten sachlich-gegenständlichen Schutzbereich von Art. 10 GG, nur diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken (§§ 100 b Abs. 3, 100 g Abs. 1 StPO).

4. Die §§ 100 a, b StPO gestatten sowohl die Erhebung der so genannten Inhaltsdaten als auch der damit zusammenhängenden Verbindungsdaten (nähere Umstände der Telekommunikation). Diese Vorschriften müssen nur beziehungsweise stets dann herangezogen werden, wenn Inhaltsdaten erhoben werden sollen.

5. Die §§ 100 g, h StPO erlauben hingegen nur die Erhebung von Verbindungsdaten, mithin der näheren Umstände der Telekommunikation. Die vom Geltungsbereich dieser Vorschrift erfassten Daten sind in deren Abs. 3 enumerativ, das heißt abschließend aufgezählt.

6. Sofern ein Datum dem Anwendungsbereich der §§ 100 g, h StPO unterfällt, besteht nach Eingang eines Auskunftsersuchens der Bedarfsträger gemäß § 3 Abs. 1 TDSV eine Speicherverpflichtung bis zur Auskunftserteilung.

7. Nach dem vorrangig aus Art. 10 GG, den §§ 100 a, b, g und h, den §§ 39 ff. AWG sowie dem G10-Gesetz herzuleitenden Telekommunikationsbegriff unterfallen diesem allein Nachrichteninhalte, mithin menschliche Verständigungsvorgänge. Hierzu zählen indes nicht die „Stand-by"-Daten eines Handys als lediglich „technisch bedingte Spuren der Kommunikationsbereitschaft" (vgl. statt vieler Weßlau, NStW Bd. 113, S. 681, 690).

8. Die Angaben zum Standort eines lediglich „aktiv geschalteten", also eines nicht telefonierenden Mobiltelefons könnten danach von den Bedarfsträgern losgelöst von den Voraussetzungen der §§ 100 a, b, g und h StPO, mithin auf der Grundlage der allgemeinen Vorschriften erhoben werden.

9. Auch § 100 i StPO ermöglicht unter anderem die Standortbestimmung eines „aktiv geschalteten Mobilfunkendgerätes". Der Gesetzgeber ist hier entweder davon ausgegangen, dass damit kein Eingriff in Art. 10 GG verbunden oder aber dessen Zitierung nicht erforderlich gewesen ist. Jedenfalls verweist das Gesetz vom 6. 8. 2002 (BGBl. I S. 3018), mit welchem § 100 i in die StPO eingeführt worden war, zutreffend nicht auf Art. 10 GG. Sein Schutzbereich dürfte nicht berührt sein. Anders als die §§ 100 a, g StPO ermöglicht § 100 i StPO die Erhebung telekommunikationsrelevanter Daten mittels des Einsatzes technischer Mittel ohne Inanspruchnahme der Diensteanbieter.

Auch werden die entsprechenden Daten nicht „im Falle einer Verbindung“ erhoben. Dies geht unter anderem aus der Regelung in § 100 i Abs. 1 Nr. 2 StPO hervor, der lediglich die Ermittlung des Standorts eines „aktiv geschalteten Mobilfunkendgerätes“, das heißt eines nicht telefonierenden Mobilfunkendgerätes gestattet. § 100 i Abs. 1 Nr. 2 StPO kann mithin als die Regelung eines speziellen Falls der Observation durch den Einsatz technischer Mittel gem. § 100 c Abs. 1 Nr. 1 b StPO und, sollten auch dessen Voraussetzungen im Hinblick auf die Dauer der Observation gegeben sein, gem. § 163 f StPO (längerfristige Observation) angesehen werden. Er schränkt die Möglichkeiten dieser Normen indes insoweit ein, als die Erfassung der „Stand-by-Daten“ eines Mobiltelefons nicht zur weiteren Erforschung des Sachverhalts, sondern lediglich zur vorläufigen Festnahme nach § 127 Abs. 2 StPO oder zur Ergreifung des Täters aufgrund eines Haftbefehls oder Unterbringungsbefehls statthaft ist.

10. Die §§ 89 Abs. 6, 90 TKG gestatten die Erhebung von Bestands- und Kundendaten. Sie gehen insoweit über die allgemeinen Vorschriften, etwa die der §§ 161, 161 a, 163 beziehungsweise §§ 94, 110 StPO hinaus, als sie eine Mitwirkungspflicht der Diensteanbieter begründen.

11. Die §§ 100 g StPO und 90 TKG haben eine gemeinsame Teilmenge, nämlich unter anderem die Rufnummer. Ob diese als Verbindungs- oder aber als Kundendatum anzusehen ist, hängt einzig davon ab, ob sie „im Falle einer Verbindung“ (vgl. § 100 g Abs. 3 Nr. 1 StPO) erhoben wird.

12. Soweit die vorgenannten Normen nicht einschlägig sind, bleiben die allgemeinen Regelungen unberührt.

11 Rechtsbehelfe der Service-Provider

Eine erhebliche Belastung für die Justiz stellen die zahlreichen Beschwerden der Service-Provider dar, mit denen diese die materiellrechtlichen Eingriffsvoraussetzungen überprüfen lassen wollen.

Nach der Rechtsprechung zahlreicher Landgerichte sowie der Entscheidung des Ermittlungsrichters beim BGH vom 7. 9. 1998–2 BGs 211/98 (CR 1998, S. 738, 739) sind die Diensteanbieter als Verpflichtete gem. §§ 100 a, b, 100 g, h StPO indes nicht beschwerdebefugt.

In den landgerichtlichen Entscheidungen wird insoweit ausgeführt, die Telekommunikationsbetreiber hätten lediglich zu prüfen, ob die formellen Voraussetzungen einer Überwachungsanordnung vorlägen. Insoweit dürfte ihnen eine Beschwerdebefugnis zustehen. Ein inhaltliches Prüfungsrecht stehe ihnen hingegen nicht zu. Entsprechende Beschwerden, die sich auf die Überprüfung der materiellen Voraussetzungen einer Eingriffsnorm in das Fernmeldegeheimnis beziehen würden, seien daher unzulässig.

Noch weiter geht die vorstehend zitierte Entscheidung des Ermittlungsrichters beim BGH. Dort ist die Frage, ob die Beschwerde eines Netzbetreibers „ausnahmsweise doch statthaft sein kann“ offen gelassen und darauf hingewiesen worden, dass dem kraft Gesetz zur Ausführung der Maßnahme verpflichteten Betreibern nicht die Befugnis zustehen könne, die Wirksamkeit der Anordnung zur Überwachung der Telekommunikation anzugreifen. Der Betreiber würde sich in derartigen Fällen gleichsam die Interessen des von der Überwachungsmaßnahme in erster Linie betroffenen Beschuldigten wahrnehmen, um auf diesem Weg mittelbar eigene Rechte und Interessen durchzusetzen. Dies würde zu einer Behinderung der Ermittlungsbehörden führen und nicht dem Regelungswerk des Gesetzes entsprechen, welches den Ermittlungsbehörden unter den Voraussetzungen der §§ 100 a, b StPO den sofortigen Zugriff auf die Telekommunikation gestatte.

12 Kritik der Diensteanbieter

Die Diensteanbieter beklagen im Hinblick auf die Zusammenarbeit mit der Strafverfolgung regelmäßig folgende Umstände:

1. Die verstärkte Zunahme von Maßnahmen sowohl nach §§ 100 a, b als auch nach §§ 100 g, h StPO und damit der hierfür aufzuwendenden Kosten.
2. In nahezu sämtlichen Fällen würden die Maßnahme beziehungsweise die Auskunftsersuchen als besonders dringlich dargestellt, so dass eine Sortierung der Anträge nach besonders eilbedürftigen und weniger eilbedürftigen nicht mehr möglich sei.
3. Die geltenden Regelungen zur Entschädigung seien unzureichend und ermöglichten im Einzelfall keine kostendeckende Umsetzung der Maßnahme.
4. Die übersandten Beschlüsse beziehungsweise Anordnungen genügten häufig nicht dem formalen Mindeststandard. Hierdurch sei ein erheblicher Mehraufwand erforderlich.

Diese sowie weitere Aspekte wurden durch die ZOK sowohl im bundesweiten Gremium der OK-Koordinatoren der Generalstaatsanwaltschaften anlässlich der Arbeitstagung vom 26. bis 28. 5. 2003 in Esslingen thematisiert als auch auf der ZOK-Arbeitstagung mit den OK-Koordinatoren der Generalstaatsanwaltschaften, den OK-Dezernentinnen/-Dezernenten der Staatsanwaltschaften sowie den Leitenden Beamten/Beamtinnen der Polizei-, Justizvollzugs-, Finanz- sowie der Zollfahndungsbehörden in Niedersachsen am 19./20. 11. 2003 in Celle. Ziel war, die Strafverfolgungsbehörden für die Belange der Service-Provider zu sensibilisieren.

13 Kommunikationsbedarf

Wie an der vorstehend aufgezeigten IMEI-Problematik deutlich wird, stehen Tatsachen, die für die Bewertung telekommunikationsrechtlicher Aspekte von Bedeutung sein können, nicht selten allein im Wissen der Service-Provider. Damit stellt sich die Frage, ob für die spezifischen Bedürfnisse in der Zusammenarbeit der Strafverfolgung mit den Service-Providern nicht eine Kommunikationsebene zwischen Vertretern der Landesjustizverwaltungen und der Service-Provider geschaffen werden sollte.

Dass es ein solches Bedürfnis gibt, geht aus Stellungnahmen von und Gesprächen mit Vertretern einzelner Service-Provider eindeutig hervor.

Der Bundesbeauftragte für den Datenschutz hat sich freundlicherweise bereit erklärt, gegebenenfalls Anfang des nächsten Jahres eine entsprechende „Kick-Off"-Veranstaltung zu moderieren. Aber auch die ZOK erwägt, in Absprache mit den übrigen Generalstaatsanwaltschaften, eine entsprechende Tagung durchzuführen.

14 Empfehlungen

Empfehlenswert erscheinen mir die nachfolgenden Aspekte:

1. Schaffung von Normenklarheit beziehungsweise Handlungssicherheit bezüglich
   - der Möglichkeit einer IMEI-bezogenen Telekommunikationsüberwachung,
   - der Erhebung von „Stand-by-Daten" eines nur aktiv geschalteten Mobilfunkendgerätes bei gleichzeitiger Auskunftsverpflichtung der Diensteanbieter (§§ 2 Nr. 6 TKÜV, 100 g, h StPO sind hier nicht einschlägig),
   - des Anwendungsbereichs von § 100 g Abs. 1 StPO im Hinblick auf die Abgrenzung des Merkmals „Straftat von erheblicher Bedeutung" vom Katalog des § 100 a StPO,
   - des Umstandes, dass die §§ 100 g, h StPO in Verbindung mit § 3 Abs. 1 TDSV auch dann eine zukünftige Speicherpflicht begründen, wenn ein Datum seinem sachlichen Anwendungsbereich unterfällt, ein Auskunftsersuchen der Bedarfsträger eingegangen ist und der Diensteanbieter allein aus betrieblichen Gründen eine Speicherung nicht veranlassen würde,
   - der Unzulässigkeit der Verwendung von sondertarifierten Rufnummern für Rückfragen bei TKÜ-Maßnahmen.
2. Verpflichtung der Provider zu einer Online-Übermittlung von Verbindungsdaten.

3. Einheitliche Rechtsprechung bezüglich der Unzulässigkeit von Beschwerden der Diensteanbieter, soweit es materiell-rechtliche Aspekte betrifft.
4. Novellierungen der TKÜV sollten künftig von der Zustimmung des Bundesrates abhängig sein.
5. Schaffung einer gesetzlichen Verpflichtung insbesondere der Netzbetreiber zur Offenlegung ihrer Netz- und Softwarekonfigurationen gegenüber der Regulierungsbehörde – soweit Bedarf besteht im Rahmen eines besonderen Geheimhaltungsverfahrens.
6. Schaffung einer neuen Kommunikationsebene zwischen Service-Providern und der Strafverfolgungsbehörden.
7. Evaluierung der durch die Diensteanbieter für TKÜ-Maßnahmen aufzuwendenden Kosten.
8. Unter Beibehaltung der Regelung des § 88 Abs. 1 TKG die Gewährleistung einer aufwandsadäquaten Entschädigung der Service-Provider (evtl. über pauschalierte Sätze; vgl. Entwurf des Kostenrechtsmodernisierungsgesetzes – KostRMoG).
9. Gewährleistung formaler Mindeststandards durch die Bedarfsträger bei Überwachungsanordnungen und Auskunftsersuchen.
10. Strengere Differenzierung bei der Einordnung derselben als „besonders eilbedürftig“.
11. Noch stärkere Abstimmung in der Bewertung telekommunikationsrechtlicher Fragen auf Länderebene und damit verbunden eine einheitlichere Meinungsäußerung gegenüber den Service-Providern.
12. Konsequentere Ahndung von Verstößen der Service-Provider durch die RegTP.

15 Schlusswort

Herr Präsident, meine Damen und Herren, die Strafverfolgungsbehörden und die Service-Provider sollten in einen vertieften Dialog eintreten. Die heutige Veranstaltung bietet dafür die geeigneten, das Wort ist schon mehrfach bemüht worden, Rahmenbedingungen. Sie ist ein „gewichtiger Stein“ auf dem Weg zu einem besseren gegenseitigen Verständnis und damit zugleich zu einer noch besseren Zusammenarbeit der Strafverfolgung mit den Service-Providern.

Ich danke Ihnen für Ihre Aufmerksamkeit.

Zur Zusammenarbeit der Strafverfolgung mit Service-Providern

Thomas Königshofen

Sehr geehrte Damen und Herren!

Wenn man von der Deutschen Telekom kommt und hier in Deutschland einen Vortrag halten soll, so hat man den Vorteil, dass man das Unternehmen, für das man tätig ist, nicht besonders vorstellen muss. Die Deutsche Telekom ist ein Begriff, und der Konzern steht für Dienstleistungen im Bereich der Informations- und Telekommunikationstechnik. Mit den vier Konzerndivisionen T-Com, T-Mobile, T-Systems und T-Online bietet das Unternehmen weltweit Telekommunikations- und Informationsdienste für Privat- und Geschäftskunden an, die vom einfachen analogen Telefonanschluss bis zu kompletten, hochkomplexen Firmen- und Behördennetzen für Sprach- und Datenkommunikation reichen.

Bevor ich aber auf die eigentliche Thematik meines Referates eingehe, möchte ich kurz meine beruflichen Berührungspunkte zum Thema „Zusammenarbeit zwischen Strafverfolgungsbehörden und Service-Providern" darstellen. Ich bin der stellvertretende (und zur Zeit kommissarische) Leiter des Bereichs Konzernsicherheit der Deutschen Telekom. Dieser Bereich hat nach seinem Geschäftsauftrag auch die Aufgabe, die Interessen des Konzerns bei der Erfüllung staatlicher Sonderauflagen zu vertreten. Zu diesen staatlichen Sonderauflagen zählen auch die gesetzlich in der Strafprozessordnung (StPO), im Telekommunikationsgesetz (TKG) und in der Telekommunikationsüberwachungs-Verordnung (TKÜV) geregelten Unterstützungs- beziehungsweise Auskunftspflichten der Telekommunikationsunternehmen bei der Beschaffung von Informationen für die Strafverfolgungsbehörden. Eine weitere Aufgabe des Bereichs Konzernsicherheit ist die Verhinderung und Verfolgung von Straftaten gegen die Telekom-Gruppe, insbesondere auch im gesamten Bereich der Computerkriminalität. Insofern hat der Bereich Konzernsicherheit eine Reihe von Schnittstellen zu den Strafverfolgungsbehörden.

Bevor ich in die Konzernsicherheit gewechselt bin, war ich der Konzerndatenschutzbeauftragte und leitete in der Rechtsabteilung des Konzerns den Fachbereich „Datenschutz, Informationssicherheit und Strafrecht". Auch in der alten Funktion hatte ich also eine Reihe von Berührungspunkten mit den Strafverfolgungsbehörden, bei denen teilweise nicht nur gemeinsame, sondern auch unterschiedliche Interessenlagen zum Tragen kamen.

Im Folgenden möchte ich deshalb sowohl auf die gemeinsamen als auch auf die teilweise unterschiedlichen Interessenlagen, die bei der Zusammenarbeit zwischen den Service-Providern und den Strafverfolgungsbehörden bestehen, eingehen und auch an Hand einiger Beispiele aus der Praxis bestimmte Problemfelder, insbesondere im Bereich der Datenkommunikation über das Internet, veranschaulichen.

Thomas Königshofen von der Deutschen Telecom hielt das Co-Referat

Doch kommen wir zunächst zu den gemeinsamen Interessen:

Die effiziente Verbrechensbekämpfung und die Verfolgung und Überführung von Straftätern ist eine Aufgabe des Staates im Interesse des Schutzes seiner Bürger. Diese staatliche Aufgabe wird in erster Linie von den Strafverfolgungsbehörden wahrgenommen und dient nicht nur dem Schutz von Privatpersonen, sondern natürlich auch dem Schutz von juristischen Personen, zum Beispiel auch dem Schutz der Telekommunikationsunternehmen wie der Deutschen Telekom. Gerade im Bereich der Computerkriminalität im weiteren Sinne sind die Service-Provider häufig Angriffen von Hackern ausgesetzt, die versuchen, Daten beziehungsweise Datenverarbeitungssysteme zu manipulieren und gegebenenfalls damit unbrauchbar zu machen. Hier ist eine enge Zusammenarbeit ganz offensichtlich von gemeinsamen Interesse, wobei diese Zusammenarbeit meines Erachtens nicht nur auf den konkreten Einzelfall bezogen erfolgen sollte, sondern auch eine gewisse Institutionalisierung (regelmäßiger Erfahrungsaustausch) erfahren könnte.

Auch in Fällen, in denen die Telekommunikationsunternehmen beziehungsweise Internet-Serviceprovider nicht selbst Opfer von Straftaten sind, sondern ihre Kunden, die über die Informations- und Telekommunikationsplattformen angegriffen werden, besteht ein ureigenes Interesse dieser Unternehmen an der Zusammenarbeit mit Strafverfolgungsbehörden. Zu denken ist hier beispielsweise an Fälle von Hacking in Kundensysteme wie zum Beispiel eine Datenverfälschung auf den Websites von Unternehmen und Behörden, aber auch an Fälle, in denen

Kunden dieser Unternehmen durch Straftäter anonym bedroht oder erpresst werden.

Weiterhin können noch die Fälle betrachtet werden, in denen Straftäter die Informations- und Telekommunikationsplattformen zur Begehung von Straftaten nutzen, zum Beispiel zur Verbreitung von Dateien/Bildern mit kinderpornographischem Inhalt über das Internet.

Schließlich gibt es auch Straftaten, bei denen der Bezug zu Informations- und Telekommunikationsdiensten überhaupt nicht gegeben ist, aber vermutet wird, dass ein Telekommunikationsunternehmen bei der Beschaffung von Informationen, die zur Aufklärung eines Tatverdachts beitragen können, behilflich sein kann. Zu denken ist hier beispielsweise an eine Überwachung des Email-Verkehrs einer Person, die im Verdacht steht, Nachrichtenmittler für einen Drogendealer zu sein, oder aber an die Auskunft eines Telekommunikationsunternehmens über die Bankverbindung eines Kunden, der im Verdacht steht, ein Geldwäschedelikt verübt zu haben.

In allen Fällen ist es im Grundsatz selbstverständlich, dass die Unternehmen, die Dienstleistungen im Telekommunikations- und Multimediabereich anbieten (Service-Provider), die Strafverfolgungsbehörden bei dem staatlichen Ziel der Verfolgung und Aufklärung von Straftaten zu unterstützen. Diese grundsätzliche Bereitschaft zur Zusammenarbeit hat aber auch genauso selbstverständlich ihre Grenzen, wo gesetzliche Regelungen konkrete Formen der Zusammenarbeit im Interesse der Freiheits- und Persönlichkeitsrechte der Bürger untersagen.

In der Praxis spielt dies insbesondere dort eine Rolle, wo die Service-Provider Informationen über ihre Kunden auf Grund ihrer vertraglichen Beziehung zu diesen Kunden vorhalten beziehungsweise beschaffen könnten, weil die Beschaffung dieser Informationen beziehungsweise ihre Bekanntgabe an Dritte (auch an Strafverfolgungsbehörden) datenschutzrechtlichen Grenzen unterliegt. So verlangen das die Service-Provider verpflichtende Telekommunikationsgeheimnis (Fernmeldegeheimnis) nach § 85 des Telekommunikationsgesetzes (TKG) und die einschlägigen Datenschutzgesetze (Bundesdatenschutzgesetz, Teledienstedatenschutzgesetz, Telekommunikationsgesetz und Telekommunikations-Datenschutzverordnung) sowohl für die Beschaffung von Daten (Erhebung) als auch für deren Weitergabe an Dritte (Übermittlung) entweder das Einverständnis der Betroffenen, also der Personen, auf die sich diese Daten beziehen, oder aber eine gesetzliche Grundlage. Auf die Grundsätze der Amtshilfe konnte man sich deshalb auch schon zu früheren Zeiten, als die Bundespost noch eine Behörde war, nicht beziehen. Heute ist dies angesichts der Tatsache, dass die Deutsche Telekom in eine privatisierte Aktiengesellschaft umgewandelt wurde, erst recht nicht möglich.

Die wichtigste gesetzliche Grundlage für die im Interesse der Strafverfolgungsbehörden durchzuführende Informationsbeschaffung mit Hilfe der Service-Pro-

vider findet sich im § 100 a Strafprozessordnung, auf dessen Basis die Überwachung der Telekommunikation zu Zwecken der Strafverfolgung angeordnet werden kann. Dem korrespondiert § 88 des Telekommunikationsgesetzes, der die Service-Provider generell verpflichtet, den Strafverfolgungsbehörden die für die Telekommunikationsüberwachung erforderlichen Netzzugänge zur Verfügung zu stellen. Die Vorschriften der §§ 100 g und h der Strafprozessordnung und § 89 Abs. 6 des Telekommunikationsgesetzes regeln die wesentlichen gesetzlichen Pflichten der Service-Provider zur Übermittlung von Kundendaten an die Strafverfolgungsbehörden.

Mit diesen grundsätzlichen gesetzlichen Pflichten sind aber auch die gesetzlichen Voraussetzungen beschrieben, die erfüllt sein müssen, damit die Service-Provider überhaupt in rechtlich zulässiger Weise die Informationen über ihre Kunden beschaffen beziehungsweise weitergeben dürfen. Die genaue Auslegung dieser Voraussetzungen war und ist häufig rechtlich umstritten, was sich dann auch auf die Praxis der Zusammenarbeit der Service-Provider mit den Strafverfolgungsbehörden niederschlägt. Diese Konfliktfelder möchte ich im folgenden an Hand von einigen Beispielen aus der Praxis erläutern.

Der erste Beispielsfall betrifft die Auskunft über den Nutzer einer dynamischen IP-Adresse.

Einem unbekannten Hacker ist es gelungen, sich durch Überwinden der Zugriffssicherung auf dem Server einer Behörde (z. B. Stadtverwaltung) schreibende Rechte für Websites zu verschaffen, deren Inhalte von der Stadtverwaltung im Internet zur Verfügung gestellt werden. Der Inhalte dieser Websites wird durch den Hacker dergestalt verändert, dass nunmehr – scheinbar in der Verantwortung der Behörde – nationalsozialistische Propaganda oder beleidigende Äußerungen auf dieser Website – für jedermann lesbar – erscheinen. Die Auswertung der Logfiles des Servers der Behörde lassen es als wahrscheinlich erscheinen, dass die Manipulation der Website von einem Internet-Anschluss ausging, dessen IP-Adresse aufgezeichnet wurde. Nach dem Adressenraum der IP-Adresse handelt es sich um eine Adresse, die von einem Access-Provider, zum Beispiel von T-Online verwaltet wird.

Bei dieser Fallkonstellation besteht unter anderem der Verdacht der Verbreitung von Propagandamitteln verfassungswidriger Organisationen im Sinne von § 86 StGB, aber auch der Verdacht einer rechtswidrigen Datenveränderung im Sinne von § 303 a StGB.

Um die Tat aufzuklären, ist die Kenntnis der Tatsache, welchem Anschlussinhaber die mitgeloggte IP-Adresse zuzuordnen ist, von entscheidender Bedeutung. Auskünfte hierüber könnte nur der Service-Provider – im Beispielsfall T-Online – geben.

Eine solche Auskunftserteilung stellt sich juristisch als Übermittlung von personenbezogenen Daten dar, die nach den einschlägigen datenschutzrechtlichen

Bestimmungen nur auf der Basis einer Einwilligung des Betroffenen oder auf einer gesetzlichen Grundlage erfolgen darf.

Eine gesetzliche Regelung über Auskunftserteilungen findet sich in § 89 Abs. 6 TKG. Nach dieser Bestimmung haben Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, personenbezogene Daten, „die sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben, im Einzelfall auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten . . . erforderlich ist."

Zunächst einmal könnte man fragen, ob ein Access-Provider, der seinen Kunden den Zugang zum Internet anbietet, überhaupt ein Telekommunikationsunternehmen oder nicht etwa ein Teledienste-Anbieter ist. Eine vergleichbare Regelung zur Auskunftspflicht und damit auch Auskunftsberechtigung der Telekommunikationsunternehmen findet sich nämlich weder im Teledienstegesetz noch im Teledienstedatenschutzgesetz. Nach § 2 Abs. 2 Nr. 3 des Teledienstegesetzes ist das Angebot zur Nutzung des Internets als Teledienst zu klassifizieren. Andererseits wird in § 2 Abs. 4 des Teledienstegesetzes klargestellt, dass das Teledienstegesetz nicht für Telekommunikationsdienste im Sinne des TKG gilt. Somit ist schon rechtlich unklar, ob die Vorschriften des Telekommunikationsgesetzes – die ja nur zur Anwendung kommen, wenn es sich um einen Telekommunikationsdienst handelt – und damit auch die Regelungen über die Auskunftspflichten nach § 89 Abs. 6 TKG im Beispielsfall überhaupt greifen.

Unterstellt man aber hier einmal, dass es sich bei dem Zugang zum Internet auch um ein Telekommunikations-Angebot im Sinne des § 3 Nr. 16 TKG (Telekommunikation im Sinne eines technischen Vorgangs „des Aussendens, Übermittelns und Empfangen von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen") handelt und damit die Anwendbarkeit des § 89 Abs. 6 TKG nicht von vornherein ausgeschlossen ist, kommt hier aber eine technische Besonderheit zum Tragen, die auch für die juristische Bewertung des Falles eine besondere Rolle spielt, nämlich die Praxis der Vergabe dynamischer IP-Adressen.

T-Online vergibt wie viele andere Access- beziehungsweise Service-Provider im Internet an seine Privatkunden regelmäßig keine festen IP-Adressen, sondern die IP-Adressen werden automatisch für jede „Session", also für jede Verbindung zum Rechner, der den Zugang zum Internet herstellt, neu vergeben. Diese so vergebenen dynamischen IP-Adressen sind also – anders als zum Beispiel fest vergebene Telefon-Nummern – keine Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben werden. Damit ist meines Erachtens die dynamische IP-Adresse nicht als so genanntes Bestandsdatum (wie z. B. der Name, die Telefonnummer, die Bankverbindung etc.) eines Kunden zu werten.

Da die dynamischen IP-Adressen einem Kunden nur für eine bestimmte Session zugeordnet werden können, lässt sich aus der Verbindung des temporären Nutzers dieser Adresse und der Zeit, für die diese Adresse vergeben wurde, herleiten, von welchem Anschluss eines Nutzers aus wann und wie lange eine Verbindung zum Internet bestanden hat. Nach § 6 Abs. 1 des Teledienstedatenschutzgesetzes sind Nutzungsdaten insbesondere Merkmale zur Identifikation des Nutzers und Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung. Es spricht somit vieles dafür, die dynamischen IP-Adressen als Nutzungsdaten im Sinne des § 6 des Teledienstedatenschutzgesetzes anzusehen. Sie können aber ebenso gut als Verbindungsdaten im Sinne der Telekommunikationsvorschriften angesehen werden, denn diese sind nach § 2 Nr. 4 der Telekommunikations-Datenschutzverordnung als „personenbezogene Daten eines an der Telekommunikation Beteiligten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden", definiert.[1]

Unabhängig von der Frage der Qualifikation des Angebots eines Access-Providers als Teledienst oder (auch) Telekommunikationsdienst scheidet somit § 89 Abs. 6 TKG als Rechtsgrundlage für die Übermittlung des Namens eines Kunden, für dessen Anschluss zu einem bestimmten Zeitpunkt eine dynamische IP-Adresse vergeben war, meines Erachtens aus.

Es bleibt aber die Möglichkeit nach § 100 g der Strafprozessordnung eine Auskunftsanordnung zu erlassen. Diese Anordnung kann von einem Richter – bei Gefahr in Verzug auch von einem Staatsanwalt – unter anderem dann erlassen werden, wenn der Verdacht besteht, dass jemand als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung oder mittels einer Telekommunikations-Endeinrichtung begangen hat. Auskunftspflichtig sind die Unternehmen, die geschäftsmäßig Telekommunikationsdienste im Sinne des TKG erbringen oder daran mitwirken. Auskunft ist hier zu erteilen über Telekommunikationsverbindungsdaten, wozu nach Abs. 3 des § 100 g StPO unter anderem Berechtigungskennungen sowie Rufnummern bzw. Kennungen der angerufenen oder anrufenden Anschlüsse oder der Endeinrichtungen gehören.

Unterstellt man auch insoweit für den konkreten Fall, dass hier die Voraussetzungen einer Anordnung nach § 100 g StPO erfüllt sind, dann könnte die Strafverfolgungsbehörde mit Aussicht auf Erfolg den Täter ermitteln, wenn der Access-Provider die Zuordnung der dynamischen IP-Adresse zu dem jeweils nutzenden Kunden auch über das Ende der Session hinaus weiterspeichert. Die Zulässigkeit der Weiterspeicherung dieser Daten durch die Access-Provider ist allerdings datenschutzrechtlich höchst umstritten. Insbesondere im Bereich der so genannten Flatrate-Angebote, bei denen die Kunden nutzungsunabhängig einen bestimmten Pauschalbetrag bezahlen, wird häufig in Frage gestellt, ob hier eine Weiterspei-

1 Vgl. hierzu Königshofen, TDSV-Kommentar, zu § 2 TDSV, Rn. 10 m. w. N.

cherung der Daten zum Nachweis der Richtigkeit der Abrechnung überhaupt zulässig ist.

Das Regierungspräsidium Darmstadt als die für T-Online im Rahmen der Erbringung von Telediensten zuständige Datenschutzaufsichtsbehörde hat die gegenwärtige Praxis der T-Online AG, wonach die Zuordnung der dynamischen IP-Adresse zu einem bestimmten Kunden grundsätzlich für 80 Tage ab Rechnungsstellung weitergespeichert bleibt, meines Erachtens richtigerweise für zulässig erachtet.[2] Insofern würde nach der jetzigen Praxis im Beispielsfall eine entsprechende Anordnung an T-Online wahrscheinlich im Ergebnis die für die Strafverfolgung entscheidenden Hinweise ergeben.

Dieser Fall zeigt aber auch deutlich, dass die Rechtslage alles andere als eindeutig ist, was sowohl für Strafverfolgungsbehörden als auch für Service-Provider eine unbefriedigende Situation darstellt.

Ein weiterer Beispielsfall, in dem das BKA unmittelbar beteiligt war, soll die Problematik zusätzlich beleuchten:

Ein vom Bundeswirtschaftsministerium gefördertes Projekt des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) und der Technischen Universität Dresden mit dem Projektnamen AN.ON betreibt einen Anonymisierungsdienst im Internet, der gewährleisten soll, dass sich Internet-Nutzer im Netz vollständig anonym bewegen können.

Bei einem Verdachtsfall im Bereich der Kinderpornographie hatte das Amtsgericht Frankfurt auf Antrag des BKA eine Anordnung nach § 100 g StPO erlassen, wonach die Projektpartner verpflichtet wurden, Auskunft über die zukünftige Telekommunikation für eine näher bestimmte IP-Adresse zu erteilen. Die Projektpartner folgten zunächst dieser Anordnung und protokollierten die entsprechenden Daten, das ULD erhob aber gegen den Beschluss des Amtsgerichts Frankfurt Beschwerde mit der Begründung, dass § 100 g StPO keine ausreichende Rechtsgrundlage für die Anordnung der Erhebung von Daten sei, sondern von dieser Vorschrift vielmehr nur die Daten erfasst würden, die seitens der Diensteanbieter auf Grund bestehender Regelungen zulässigerweise erhoben und gespeichert würden.

Dieser Rechtsauffassung war das Landgericht Frankfurt als Beschwerdeinstanz im Ergebnis gefolgt und hatte zunächst die Vollziehung der Anordnung im Eilverfahren ausgesetzt und später im Hauptsacheverfahren den angefochtenen Beschluss des Amtsgerichts aufgehoben.[3]

Auch die während des schwebenden Rechtsstreits vom Amtsgericht Frankfurt erlassene Durchsuchungsanordnung für die Räume des AN.ON-Projektes an der

2 Vgl. hierzu kritisch aber auch c't aktuell, Meldung vom 14. 1. 2003, http:/www.heise.de/ct/aktuell/meldung/33674.

3 Vgl. die Dokumentation zum Rechtsstreit AN.ON in DuD 2003, S. 711 ff.

Technischen Universität Bremen, die das Ziel hatte, die Protokolldatensätze sicherzustellen, wurde vom Landgericht Frankfurt für rechtswidrig erachtet und mit der Begründung aufgehoben, diese Durchsuchungsanordnung stelle eine rechtsmissbräuchliche Umgehung des Beschlusses des Landgerichts dar, mit dem die Vollziehung der Auskunftsverpflichtung ausgesetzt worden war.[4]

Auch dieses Beispiel zeigt die hohe Rechtsunsicherheit im Rahmen der gesetzlichen Regelungen für Auskunftsverlangen zu Strafverfolgungszwecken im Bereich der Internet-Nutzung.

Jedoch sei an dieser Stelle darauf hingewiesen, dass jedenfalls die Vorschrift des § 100 a StPO, die die Voraussetzungen für die Anordnung der Telekommunikationsüberwachung regelt, anders als § 100 g StPO auch eine Verpflichtung zur Datenspeicherung in den Fällen enthält, in denen ansonsten von den Service-Providern keine Daten gespeichert werden.

Allerdings ist die Anwendung des § 100 a StPO auf Ermittlungsfälle beschränkt, die unter die dort genannten Katalogstraftaten zu subsumieren sind. In Betracht käme insoweit im beschriebenen Fall nur der Verdacht der Verbreitung pornographischer Schriften im Sinne des § 184 Abs. 4 StGB, was wiederum den qualifizierten Verdacht voraussetzt, dass die pornographischen Schriften nicht nur den sexuellen Missbrauch von Kindern zum Gegenstand haben, sondern auch ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben müssen. Dies kann möglicherweise im Einzelfall bei zwar eindeutig pornographischen Bildern von Kindern, die aber kein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben, dazu führen, dass nach der gegenwärtigen Rechtslage bei einfachen Delikten der Kinderpornographie eine in die Zukunft gerichtete Anordnung zur Datenspeicherung ohne Erfolg bliebe. Um dieses Ergebnis zu vermeiden, wäre aber eine Regelung de lege ferenda, die die Service-Provider verpflichten würde, ohne jeden Anfangsverdacht und betriebliche Notwendigkeit sämtliche Verbindungsdaten aller Kunden beziehungsweise Nutzer für eine bestimmte Zeit zu speichern (so genannte „Vorratsdatenspeicherung“, international auch „data retention“ genannt), nicht erforderlich. Sie würde auch sehr stark in die Persönlichkeitsrechte und das Grundrecht auf Wahrung des Fernmeldegeheimnisses eingreifen.

In diesem speziellen Fall wäre eine moderate Erweiterung des § 100 a StPO im Hinblick auf die erfassten Katalogstraftaten (z. B. eine Einbeziehung des § 184 Abs. 3 StGB in den Straftatenkatalog) ausreichend, wenn man dem Phänomen der Verbreitung von Kinderpornographie im Internet wirksamer begegnen will.

Letztlich ist aber auch dies eine Entscheidung des Gesetzgebers, der zwischen den Interessen der Bürger an einer effektiven Strafverfolgung und den Interessen der Bürger auf Schutz ihrer Privatsphäre bei der Nutzung der modernen Informa-

4 Pressemitteilung des ULD SH vom 4. November 2003.

tions- und Kommunikationsmittel abzuwägen und hier gegebenenfalls einen vernünftigen und verhältnismäßigen Interessenausgleich anzustreben hat. Dabei darf der Schutz der Privatsphäre der Bürger nicht polemisch als „Täterschutz" diffamiert werden, denn die betrieblich nicht notwendige Speicherung der Daten über das Telefonierverhalten (wer hat wann mit wem telefoniert?) und das Nutzungsverhalten im Internet (wer hat wann und wie lange welche Websites angeschaut?) auf Vorrat trifft ja nicht nur diejenigen, die im Verdacht stehen, eine Straftat begangen zu haben, sondern jedermann, vom Journalisten bis zum Abgeordneten und von der Schwangerschaftsberaterin bis zum Polizeipräsidenten.

Unabhängig von der jeweiligen persönlichen Position zu dieser Frage kann aber auch insoweit festgehalten werden, dass der Gesetzgeber sich im Interesse der Rechtssicherheit um klare und eindeutige Regelungen bemühen muss, da dies die Voraussetzung für eine weitgehend konfliktfreie und reibungslose Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Service-Providern ist.

Ein weiteres Konfliktfeld zwischen den Strafverfolgungsbehörden und den Unternehmen der Informations- und Telekommunikationsbranche, das hier nicht verschwiegen werden soll, kann sich aus der einfachen Tatsache ergeben, dass die Zuarbeit für die Strafverfolgungsbehörden organisatorische, personelle und sachliche Mittel erfordert, die nach den derzeitigen gesetzlichen Bestimmungen beziehungsweise nach der herrschenden Auslegung der einschlägigen Bestimmungen durch die Gerichte auch nicht annähernd durch einen Kostenersatz von Seiten staatlicher Stellen ausgeglichen wird.

So müssen von den Telekommunikationsunternehmen für die Vorhaltung und den Betrieb von technischen Einrichtungen zur Ermöglichung von Überwachungsmaßnahmen jährlich Millionenbeträge ausgegeben werden. Nach einer BDI-internen Umfrage[5] werden in Deutschland derzeit nur durchschnittlich 2 % der anfallenden Kosten erstattet, so dass jedes einzelne Unternehmen Belastungen in zwei- bis dreistelliger Millionenhöhe zu tragen hat. Die damit praktisch erfolgende entschädigungslose Indienstnahme Privater ist verfassungsrechtlich höchst problematisch.[6] In diesem Zusammenhang verdient auch eine Entscheidung des österreichischen Verfassungsgerichtshofes besondere Beachtung. Dieser hat kürzlich die in Österreich geltende gesetzliche Kostenregelung, die mit der deutschen Rechtslage weitgehend vergleichbar ist, für verfassungswidrig erklärt.[7]

Die einseitige Abwälzung der Kosten der Mithilfe zur Strafverfolgung auf die Telekommunikationsunternehmen kann insbesondere im internationalen Wettbewerb zu Nachteilen führen, weil die ausländischen Wettbewerber auf ihren Hei-

5 Vgl. das BDI-Positionspaper „Telekommunikationsüberwachung verfassungsgemäß und wirtschaftsfreundlich gestalten" vom 7. 10. 2003, http:/www.bdi-online.de.

6 Vgl. z. B. Koenig/Koch/Braun, K&R 2002, S. 289 ff.

7 Urteil des österreichischen VfGH (Az. G37/02), http:/www.ris.bka.gv.at/vfgh.

matmärkten nicht mit entsprechenden Kosten belastet sind. Nach einer Studie des Wissenschaftlichen Instituts für Kommunikationsdienste vom April 2003 werden in anderen europäischen und angloamerikanischen Ländern sowohl die Kosten für die netzseitigen technischen und organisatorischen Vorkehrungen als auch die Kosten für die Übermittlung an die berechtigten Stellen umfassend erstattet.[8]

Da die Telekommunikationsunternehmen – anders als die Strafverfolgungsbehörden – nicht durch Steuern finanziert werden, sondern langfristig Gewinne erwirtschaften müssen, um zu überleben, liegt es auf der Hand, dass das Verständnis für die Interessen der Strafverfolgungsbehörden an einer umfassenden und wenn nötig sehr kurzfristigen Zuarbeit durch die Telekommunikationsunternehmen dort auf Grenzen stößt, wo dies durch diese Unternehmen nur noch mit unverhältnismäßig hohen Personal- und Sachkostenbelastungen leistbar wäre.

Ebenso wie bei der Frage der Personal- und Finanzausstattung der Strafverfolgungsbehörden ist es meines Erachtens auch hier eine Entscheidung des Gesetzgebers, wie viel Steuermittel er für eine Steigerung der Effektivität der Strafverfolgung aus den staatlichen Gesamteinnahmen abzweigen will. Insofern dürfte auch die Forderung der deutschen Telekommunikationsindustrie nach einer angemessenen Kostenerstattung für die Unternehmen, die die Strafverfolgungsbehörden bei der Verbrechensaufklärung und -bekämpfung unterstützen[9], nicht auf Widerstand der Strafverfolgungsbehörden stoßen. Ich sehe auch hier eher eine gemeinsame Interessenlage als Divergenzen.

Ich komme zum Fazit:

Die gelegentlich vorgetragene Auffassung, dass die Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Unternehmen der Informations- und Telekommunikationsbranche in der Praxis nicht vernünftig funktioniere, kann ich persönlich auf Grund meiner beruflichen Erfahrungen bei der Deutschen Telekom AG nicht teilen.

Selbstverständlich gibt es Einzelfälle, wo mal etwas nicht gut gelaufen ist. Aber das halte ich angesichts der Vielzahl der Verfahren für normal, und ich habe auch die Erfahrung gemacht, dass die Fehler nicht immer nur von einer Seite produziert werden.

Die nicht immer klare Rechtslage kann aber auch dazu führen, dass zwischen den Strafverfolgungsbehörden und den Serviceprovidern unterschiedliche Rechtsauffassungen bezüglich der Anwendung und Reichweite von Vorschriften bestehen, die die Kompetenzen der Strafverfolgungsbehörden einerseits und die Rechtspflichten der Serviceprovider andererseits bestimmen. Hier gilt es meines Erach-

8 Wik-Consult-Studie: „Rechtlicher Rahmen für das Angebot von TK-Diensten und den Betrieb von TK-Anlagen in den G7-Staaten in Bezug auf die Sicherstellung der Überwachbarkeit der Telekommunikation, http:/www.wik.org."

9 Siehe die Stellungnahme des BDI vom 7. 11. 2003 zum Regierungsentwurf (Stand: 15. Oktober 2003) für ein neues Telekommunikationsgesetz (TK), S. 4 ff. (http:/www.bdi-online.de).

tens, Verständnis für die unterschiedlichen Rechtspositionen auf beiden Seiten zu entwickeln, ohne zu unterstellen, die jeweilige Seite würde mutwillig und bewusst die Interessen der jeweils anderen Seite missachten. Meine Erfahrung zeigt, dass sich dann viele Einzelfälle durch Kompromisslösungen beziehungsweise Alternativen regeln lassen. Bleiben dennoch im Einzelfall unterschiedliche Rechtsauffassungen bestehen, so sind hier zunächst die Gerichte berufen, diese Rechtsstreitigkeiten zu schlichten.

Ebenso wenig wie man den Strafverfolgungsbehörden vorwerfen sollte, dass sie die ganze Bandbreite ihrer rechtlichen Möglichkeiten im Interesse der Kriminalitätsbekämpfung – gegebenenfalls auch auf Kosten der Telekommunikationsunternehmen – ausschöpfen (das ist schließlich ihre Pflicht), sollte man den Telekommunikationsunternehmen auch keine versuchte Strafvereitelung unterstellen, wenn sie den einen oder anderen Beschluss von Staatsanwälten nicht nachvollziehen können und noch einmal gerichtlich überprüfen lassen.

Im Ergebnis ist allen mit einer höheren Rechtssicherheit geholfen. Hierfür sind klare und eindeutige gesetzliche Regelungen erforderlich, die so wenig Interpretations- und Auslegungsspielräume wie gerade rechtstechnisch möglich zulassen. Die derzeitige Gesetzeslage kann meines Erachtens dieses Kompliment nicht für sich beanspruchen. Es bleibt deshalb die Aufgabe des Gesetzgebers, bei zukünftigen Gesetzesänderungen gerade in diesem gesellschaftlich und ordnungspolitisch besonders sensiblen Bereich, diese Rechtsklarheit anzustreben.

Bis dahin sollte sich die Praxis dahingehend helfen, dass Problemfälle im Bereich der Zusammenarbeit zwischen den Strafverfolgungsbehörden und den Telekommunikationsunternehmen in der Atmosphäre eines konstruktiven Dialogs angegangen werden.

Für eine Intensivierung dieses Dialogs mit dem Ziel der Verbesserung der Zusammenarbeit steht die Deutsche Telekom jederzeit zur Verfügung.

Ich bedanke mich für Ihre Aufmerksamkeit.

Der britische Ansatz zur Kooperation zwischen Polizei und Wirtschaft und Erfahrungen mit der internationalen polizeilichen Zusammenarbeit

Len Hynds

Zunächst möchte ich mich entschuldigen, dass ich nicht auf Deutsch zu Ihnen spreche. Mein Deutsch ist sehr begrenzt. Wenn Sie es kennen würden, würden Sie verstehen, weswegen ich in Englisch zu Ihnen rede heute.

Zuerst möchte ich Folgendes sagen: Das Thema, mit dem wir uns hier befassen, ist ein unermesslich weites Thema. Und es ist unmöglich, alles hier im Detail mit Ihnen zu besprechen. Deswegen wird es so etwas wie eine Art Stippvisite sein, die ich machen werde. Ich werde hier und dort verweilen, einzelne Aspekte des Themas näher beleuchten. Gleichzeitig ist es mir wichtig, Sie gleich zu Beginn meines Vortrages wissen zu lassen, dass der rote Faden meines Vortrages die Sensibilisierung der Entscheidungsträger, sowohl im öffentlichen als auch im privaten Bereich, sein wird.

Ich möchte Sie kurz auf eine kleine Reise mitnehmen. Stellen Sie sich einmal vor, dass sich Regierungen überall auf der Welt entscheiden würden, das Internet zu einem Marktplatz für jedermann zu machen, es sozusagen zum Mainstream werden zu lassen. Das würde heißen, dass wir einen Zusammenschluss der Kommunikationsdienste erleben von ISP und IT-Industrie und dass wir alle näher zusammenrücken würden. Das bietet natürlich Vorteile, aber auch Herausforderungen und möglicherweise Risiken. Es geht nämlich darum, auch die Herausforderungen tatsächlich in Besitz zu nehmen als Bedarfsträger. Ich höre oft, wenn wir von High-Tech-Crime sprechen, die Aussage: Das ist doch das Problem der anderen. Und gleichzeitig, wenn ich meine Kollegen frage, sagen die mir: Das ist was für Experten. Da müssen Fachleute ran. Und gleichzeitig sagen sie, das sei nicht ihre eigentliche Kernaufgabe. Es gibt natürlich Parallelen auch zur Industrie. Denn dort ist in den Aufsichtsräten, Führungsgremien, teilweise die gleiche Einschätzung verbreitet. Wir müssen diese Ansichten in Frage stellen, müssen die Vertreter herausfordern, sowohl auf Seiten der Strafverfolgungsbehörden als auch auf Seiten der Industrie. Warum? Wir sprechen nämlich im Wesentlichen über Kriminalität. Da kommt natürlich jetzt noch das Etikett „High-Tech“ dazu. Das wird sozusagen aufgeklebt. Also, wir kleben dieses Etikett „High-Tech“ auf und dann müssen wir aufpassen, dass wir uns nicht in der falschen Sicherheit wiegen, dass dieses High-Tech-Element nur an der Peripherie auftaucht. Dann sitzen wir nämlich in der Falle. Dann nehmen wir das Problem, die Fragestellung als solches, nicht in Besitz. Und es geht auch bei „High-Tech-Crime“ nicht um die Technologie. Es geht um Menschen letztendlich. Wenn Menschen Opfer einer Straftat werden – sei es Erpressung, Betrug oder einer anderen Straftat im Cyberspace – dann tut das genauso weh wie wenn es eine Straftat herkömmlicher Art wäre. Um das Ganze jetzt in einen größeren Kontext zu stellen, möchte ich sagen, dass ich

drei Themenbereiche eingehender behandeln werde, also drei längere Stippvisiten machen werde, um im Bild zu bleiben.

Das heißt zunächst, dass ich überhaupt das Problem als solches beschreiben, umreißen möchte. Ich denke, das ist nützlich, dies am Anfang zu tun. Ich weiß, dass ich hier vor Experten spreche. Aber nichtsdestotrotz ist es immer gut, im Blick zu behalten: Was ist eigentlich die Definition, mit der wir arbeiten, wenn wir von Cybercrime sprechen? Dann werde ich einen Großteil meiner Zeit darauf verwenden, Ihnen etwas darüber zu berichten, wie wir uns organisiert, wie wir uns gerüstet haben, um diesem Phänomen zu begegnen. Und dann in einem dritten Teil werde ich mich darauf konzentrieren, Ihnen etwas dazu zu sagen, wie wir mit unseren Partnern in Interaktion sind, sowohl auf lokaler, nationaler als auch auf internationaler Ebene.

Ein prominenter Gast aus dem Vereinigten Königreich: Len Hynds vom NHTCU

Was meinen wir also, wenn wir von „High-Tech-Crime“ sprechen? Wir sind geneigt, Straftaten zu kategorisieren. Ich denke, das ist auch für Sie ein bekanntes Phänomen. Wir sprechen von alten traditionellen Straftaten. Und die tauchen jetzt in einem neuen Gewand auf. Und dieses neue Gewand heißt Internet. Und dann gibt es natürlich auch neue Straftaten, neue Phänomene: Hacking, Cracking, Virus. Ich denke, wir sollten etwas vorsichtiger sein, was den Sprachgebrauch angeht und unterscheiden zwischen den Straftaten, die altbekannt sind, die lediglich in diesem neuen Gewand auftauchen, und den Straftaten, die nicht begangen wer-

den unter Nutzung dieser neuen Medien. Das heißt, wir müssen unterscheiden zwischen diesem erschwerenden Element, das hinzukommt, nämlich das Tatmittel, das eingesetzt wird: das Internet. Wir müssen die Definitionen, mit denen wir bisher gearbeitet haben, in Frage stellen. Und das ist etwas, was nicht nur das Vereinigte Königreich betrifft. Wir müssen diese Definitionen hinterfragen, die sich natürlich bewährt haben und an denen Menschen aber nach wie vor festhalten.

Es scheint doch nach wie vor so zu sein, dass man vor dem Gedanken zurückschreckt, irgendwie physisch in ein Büro einzubrechen und etwas zu entwenden. Aber wenn das Ganze über das Internet abgewickelt wird, also Hacking-Angriffe gefahren werden, dann liegen die Hemmschwellen ganz woanders. Und da müssen wir ein Umdenken in Gang setzen. Ich zeige Ihnen jetzt hier eine Definition, was man unter „Cybercrime" versteht. Und wenn Sie da hinschauen, werden Sie vielleicht merken: Die Definition ist nicht allumfassend. Der Grund hierfür ist folgender. Es handelt sich um eine Definition der Wirtschaft. Das ist die Definition der Wirtschaft von Cybercrime. Und hier müssen wir das erste Mal kritische Fragen stellen. Ich glaube, wir als Strafverfolgungsbehörden müssen Strategien entwickeln, mit Definitionen arbeiten, die wir selbst erarbeitet und entwickelt haben. Wenn wir das Problem aus unserer Sichtweise definieren, dann können wir auch die Risiken, die Herausforderungen besser einschätzen und uns dagegen wappnen.

Bevor wir jetzt diese Liste in Grund und Boden verdammen und sagen: „die ist irrelevant", sollten wir aber Folgendes bedenken. Wir haben verlässliche Informationen vorliegen, die besagen, dass Rauschgifthändlerringe, Waffenhändler beispielsweise, sich immer stärker auf das Internet verlegen, arbeiten mit, verkehren über Internet Relay Chats, nutzen ICQ Protocols und verschlüsseln ihren Nachrichtenverkehr. Es finden Hacking-Angriffe statt. Und gleichzeitig wird das Internet auch eingesetzt, um illegale Aktivitäten der Täterseite zu verschleiern. Was ich der Wirtschaft sagen möchte, ist, dass wir mit unseren Definitionen aufeinander zugehen müssen, dass wir, dass insbesondere auch die Wirtschaft, dem Phänomen der OK eine verstärktere Beachtung schenken muss und dass die traditionelle Definition von „Opfer" erweitert werden muss. Und das wird ganz deutlich, wenn wir uns in die High-Tech-Arena begeben. Die Täterseite betätigt sich dort wie Parasiten, sucht nach Hosts im wahrsten Sinne des Wortes, wo sie sich einnisten und ihr Unwesen treiben können. Wie sieht also die Bühne aus? Welches Szenarium müssen wir für unsere Arbeit kreieren?

Es ist ein sehr komplexer und oft schwer zu fassender Phänomenbereich. Aber es gibt doch einige Elemente, die ich herausgreifen möchte. Cyberattacks können aus der Ferne geschehen. Sie geschehen unvermittelt. Der Täter sitzt irgendwo an seiner Tastatur, manipuliert ganze Datensysteme und das rund um den Erdball. Nationale Grenzen existieren schlichtweg nicht. Gleichzeitig kann sich der Täter unbemerkt auch wieder zurückziehen. Die Opfer finden wir nicht in einer eingeschränkten geographischen Region. Auch hier gibt es Opfer weltweit. Das heißt,

wir haben es mit einem globalen Problem zu tun, das nach einer globalen Lösung ruft. Das heißt, was gefordert ist, ist ein interdisziplinäres Vorgehen auf lokaler, regionaler, nationaler und internationaler Ebene. Wann immer ich in Polizeikreisen diese Thematik anspreche, bekomme ich oft die Rückmeldung, meine Aufgabe bestehe doch darin, ein Problem zu lösen, eine Straftat aufzudecken, die sich mir vor Ort stellt. So ist der Blick nicht gleich geschärft für die globale Ebene.

Aber das muss wesentlicher Bestandteil einer Gegenstrategie sein. Einerseits verbindet uns das Internet auf einmalige Art und Weise, es hat unzählige Vorteile für uns als Gesellschaft. Aber gleichzeitig birgt dies auch jede Menge Herausforderungen. Jedes Instrumentarium, so auch das Internet, birgt an sich die Möglichkeit von Straftätern genutzt zu werden. Und je wichtiger ein derartiges Instrumentarium für die Wirtschaft ist, umso wichtiger ist es möglicherweise auch für die Straftäterseite. Diese Aspekte müssen wir einbeziehen, wenn wir unsere Strategien erarbeiten und umsetzen. Im Vereinigten Königreich besteht meine Aufgabe darin, mich kritisch mit den Strategien der Regierung in diesem Bereich auseinander zu setzen. Ich habe es mit zwei Zuständigkeitsbereichen zu tun. Polizeiarbeit fällt in die Zuständigkeit des Innenministeriums. Dort ist auch die Zuständigkeit angesiedelt, einen sicheren Rahmen für Polizeiarbeit zu schaffen, allgemeine Polizeiarbeit, bei uns bekannt unter dem Stichwort „Mainstream Polices". Außerdem ist das Ministerium für Handel und Wirtschaft zuständig. Dort liegt die Zuständigkeit, dafür einen sicheren, einen optimalen Rahmen zu schaffen, für das, was wir unter E-Business verstehen. Und an dieser Schnittstelle stehen sozusagen wir: die National High Tech Crime Unit. Wir sind die Pioniere, wenn es darum geht, neue und, wie ich finde, aufregende Initiativen zu entwickeln.

Wie sieht unsere Strategie aus? Es ist eine Strategie, die ungefähr drei Jahre alt ist. Sie wird zurzeit überprüft. Als Leiter der National High Tech Crime Unit bin ich zuständig für die Entwicklung dieses Plans, die Weiterentwicklung und die Umsetzung. Die Strategie fußt auf vier Säulen. Zunächst geht es darum, ein zentrales Center of Excellence einzurichten, dann im nächsten Schritt einen Rahmen zu schaffen für die Unterstützung und Koordination des Handelns sowie für das Zusammenspiel zwischen unserer zentralen Dienststelle und den lokalen Dienststellen vor Ort. Die dritte Säule betrifft die interdisziplinäre Zusammenarbeit und die Partnerschaft mit unseren Partnerdienststellen weltweit. Das Ganze wurde aufgelegt im April 2001. Ich sagte es bereits. Wir haben einen interdisziplinären Ansatz gewählt. Auch das Budget, das uns zur Verfügung steht, ist außerordentlich: 25.000.000 Pfund wurden vom Parlament für die ersten drei Jahre bewilligt. Wir haben bewusst den multidisziplinären Ansatz gewählt und alle zuständigen Behörden eingeschlossen. Wie gesagt, wir wollen einen Center of Excellence werden, eine strategische Auswertung betreiben, Unterstützung im operativen und taktischen Bereich zur Verfügung stellen, fallbezogene Intelligence-Arbeit leisten und Best Practise Advise weitergeben. Man kann auch sagen, dass wir ein nationales Koordinationszentrum sind – auch was kritische Infrastrukturen und deren Gefährdung angeht.

Diese Strategie lässt sich untergliedern in vier verschiedene Bereiche. Zunächst geht es darum, Ergebnisse zu erzielen, die in die Strafverfolgung einfließen können. Das schließt auch digitale Beweismittel ein. Wir übernehmen die Federführung bei den Ermittlungen, können aber gleichzeitig auch lokale Dienststellen unterstützen in Abhängigkeit zur Schwere der begangenen Straftat, des Organisationsgrades der Täter und auch der geographischen Bedeutung der kriminellen Aktivitäten. Zweiter Bereich: Intelligence. Wir entwickeln sowohl strategische als auch taktische Intelligence-Produkte. Denn unsere Klientel ist vielseitig. Und wir wollen möglichst allen Wünschen und Forderungen unserer Kunden gerecht werden. Wir führen aber auch eigene Aktivitäten durch und – das bringt mich zum dritten Bereich – Tactical and Technical Support Section. Das ist sozusagen unser Schaufenster nach draußen, betrifft unser Extranet, über das wir alle Dienststellen im Land miteinander vernetzen. Dann sind wir auch zuständig für Kontakte zur Industrie. Auch dort haben wir speziell ausgebildete Mitarbeiter, die diesen Kontakt halten.

Unser Arbeitsprogramm sieht folgendermaßen aus. Wir bieten eine Reihe von Produkten an. Ein Bereich betrifft den Aufbau von Infrastruktur. Das schließt die Erarbeitung von Benchmark Standards für die Dienststellen vor Ort im ganzen Land, also in England und Wales, ein. Dann geht es um die Herausbildung von Tätigkeitsprofilen. Stichwort: Aus- und Fortbildung. Wir möchten erreichen, dass alle Beamte, die sich mit der Bekämpfung der High-Tech-Kriminalität bei uns im Land befassen, bestimmte Mindeststandards gewährleisten können. Das Extranetprojekt, das ich bereits kurz ansprach, stellt eine Art Forum dar. Dort können sich Praktiker aus dem Bereich High Tech Crime treffen und sich beispielsweise über ihre Erfahrungen austauschen. Dann haben wir gewisse Regularien aufgestellt, was die Zusammenarbeit angeht zwischen den einzelnen Dienststellen, die sich unter unserem Dach finden. Das schließt ein: die National Crime Squad, die Nachrichtendienste, auch die Vereinigung leitender Polizeibeamter und die Vertretung von „HMCE“ („Her Majesty’s Customs and Excise“ = brit. Zoll). Dann kommen noch zwei weitere nationale Dienststellen hinzu, nämlich das Infrastructure Coordination Center und das National Tactical Assistance Center.

Die Ermittlungsstandards für Ermittlungen im Bereich High-Tech-Kriminalität sind inzwischen fest verankert im Handbuch für Beamte in diesem Bereich und haben auch Eingang gefunden in das Handbuch, was die Handhabung von digitalen Beweismitteln angeht. Das heißt, unsere Arbeit hat Auswirkungen auf jede Polizeidienststelle im Land. Wir sind weiterhin beauftragt, NCS (National Crime Squad) über die Entwicklung im Bereich High Tech Crime zu unterrichten. Wir erstellen Grundsatzberichte. Das Wichtige hier ist allerdings, dass die Rohdaten bei den lokalen Dienststellen vorbehalten werden. Das heißt, dass diese Dienststellen eng mit uns zusammenarbeiten, uns zuliefern müssen und dass sie ihre Art der Informationssammlung kritisch hinterfragen und anpassen müssen. Der vierte Bereich betrifft die Partnerschaft mit der Wirtschaft und mit unseren Part-

nerdienststellen im Ausland. Das ist eine Verpflichtung, die wir eingegangen sind, die ganz wesentlich ist und sich überall niederschlägt.

Eine Reihe von Umfragen werden jedes Jahr im Vereinigten Königreich durchgeführt. Diese konzentrieren sich vorrangig auf die Perspektive der Unternehmen. Es handelt sich dabei um hervorragende Indikatoren für die Lage. Aber ich denke, unser Wissen ist immer noch lückenhaft. Wir verfolgen natürlich die Trends aufgrund der Daten, die uns zugeliefert werden. Wichtig ist, dass wir tatsächlich Zugang zu den Schlüsseldaten haben. Deshalb müssen wir uns global ausrichten, um uns dafür zu rüsten, dass die Daten zu diesem Kriminalitätsphänomen in einer Form festgehalten werden, dass sie auch für ein strategisches Lagebild weiterverarbeitet werden können und als Grundlage für die Ressourcenplanung herangezogen werden können. Man muss das wahre Ausmaß dieses Phänomens verstehen, um die Strategie neu auszurichten. Wir haben daher zwischen den Polizeikräften im Vereinigten Königreich Vereinbarungen getroffen und uns auf eine Datenerfassungsmodalität geeignet und darin auch die Aufgabe unserer Ausbildungseinrichtungen festgelegt. Diese Vereinbarung ist in erster Linie eine Arbeitsteilung, die Aufgaben innerhalb der Polizei klar festlegt und versucht, undeutliche Zuständigkeiten zu vermeiden. Das ist besonders wichtig, wenn man sich vor Augen hält, wie High-Tech-Kriminalität, IuK-Kriminalität Grenzen überschreitet.

Viele gesetzliche Grundlagen sind geschaffen worden, ohne die virtuelle Welt zu berücksichtigen. Deshalb ist es unsere Aufgabe, uns für dieses neue Phänomen zu rüsten und innerhalb der Polizei neue Routinen festzulegen. Wir berücksichtigen selbstverständlich auch offene Quellen und nutzen Strategien, die im verdeckten Bereich üblich sind. Die Ermittler im Netz haben ein neues Handbuch bekommen. Wir haben dieses Handbuch mit der Staatsanwaltschaft abgestimmt, ebenso mit den Spezialisten für Überwachungstechnologie und allen Fachdienststellen, die sich mit Computerkriminalität im Land befassen. Darüber hinaus gibt es einen Leitfaden für Computerforensiker, der ebenfalls auf den neuesten Stand gebracht wurde. In beiden Leitfäden sind Standards festgelegt für die Zusammenarbeit mit dem privaten Sektor. Wir stellen fest, dass es sich besser arbeiten lässt, wenn eine Partnerschaft zwischen Strafverfolgung und dem privaten Sektor besteht. Man kann die Dokumente unter unserer Webadresse www.nhtco.org abrufen.

Seit der Gründung unserer Fachdienststelle haben wir es uns zum Ziel gemacht, die Zusammenarbeit mit dem privaten Bereich auszubauen und mit den Verbrauchern auch eine entsprechende Öffentlichkeitsarbeit zu betreiben. Meines Erachtens können wir einen Fortschritt nur erreichen, indem wir uns um Partnerschaft bemühen. Wir haben deshalb ein spezielles Kontaktprogramm aufgelegt, in dem es darum geht, wie wir an spezielle Daten kommen, wie wir Erkenntnisse überprüfen können und was im Sinne einer Kriminalprävention geleistet werden kann. Ich bin überzeugt, dass wir von dieser Form der Partnerschaft profitieren. Nur durch Partnerschaft können wir ein wirkliches Lagebild zeichnen. Ich glaube, das ist entscheidend. Selbst wenn wir eine umfassende Sicht der Dinge haben, er-

reichen wir nur dann ein vollständiges Bild der Lage, ein vollständiges Verständnis des Phänomens, wenn wir zusammenarbeiten und verschiedene Informationsquellen zusammenführen. Wir müssen deshalb die verschiedenen Interessengruppen, die Interessen der Serviceprovider, die Telekommunikationsindustrie, die Hardware- und Softwarehersteller und natürlich auch den Finanzsektor berücksichtigen. Indem wir versuchen, die Industrie mit einzubeziehen, sehen wir uns auch vor einer großen Herausforderung. Wir verfügen jetzt über Verbindungen mit dem Arbeitgeberverband in Großbritannien, mit dem Institut der Direktoren und auch mit anderen Handelsvertretungen. Aber wir haben es immer noch nicht geschafft, den Mittelstand vollständig mit einzubeziehen. Wir müssen auch die lokale Ebene mit einbeziehen. Das versuchen wir auch durch Polizeiarbeit vor Ort zu leisten.

Ein Schlüssel für den Erfolg ist natürlich auch die internationale Zusammenarbeit. Ich glaube, dass die Strafverfolgungsgemeinschaft hier sehr viel beizutragen hat. Das ist auch eine wichtige Botschaft an die Industrie – die Vernetzung der Strafverfolgungsbehörden. In dem Interpol-Zusammenschluss befinden sich 179 Mitgliedstaaten. Europol bringt weitere 15 Staaten mit ein im europäischen Szenario. Mittlerweile haben sich 34 Länder dem G8-Übereinkommen angeschlossen, das 1997 in Washington geschlossen wurde. Wir haben Kontaktstellen eingerichtet, die rund um die Uhr verfügbar sind, um gegenseitig Unterstützung in Notfällen zu leisten. Das ist ein sehr wichtiges Hilfsmittel bei der Bekämpfung von IuK-Kriminalität in einer grenzüberschreitenden Ausprägung. Denn man muss bedenken, dass Daten sehr schnell vernichtet werden können. Deshalb ist es sehr wichtig, den so genannten Tatort schnell einzufrieren. Das ist sehr wichtig für die Strafverfolgung. Das ist vielleicht auch die einzige Möglichkeit, um hinterher an die Täter zu kommen und deren illegales Vermögen einzufrieren. Wenn der Tatort erst einmal eingefroren ist, haben wir fest vereinbarte Abläufe im Rahmen der internationalen Rechtshilfe. Dies wird durch Interpol vermittelt.

Wenn die Industrie eine eigene Strategie verfolgt, verzichtet sie auf die Möglichkeiten, die die Strafverfolgungsbehörden mit einbringen können; eine Verfolgung der Täter ist dann nicht möglich. Europol und Interpol sind die wichtigsten Partner beim Erkenntnisaustausch. Wir haben gemeinsam mit Europol sehr gute Work-Files-Auswerteprojekte durchgeführt, in denen die Analyseabteilung von Europol ihre Kapazitäten eingebracht hat. Des Weiteren ist zu erwähnen, dass sich die Leiter von IuK-Fachdienststellen regelmäßig bei Europol treffen, um sich auszutauschen. Meine Fachdienststelle ist erst vor zwei Jahren voll arbeitsfähig geworden. Aber wir haben bereits eine kleine Zahl von Fachleuten in mehr als dreißig Ländern zum Einsatz gebracht. Damit decken wir fast jeden Kontinent ab. Das zeigt unseren globalen Ansatz und die Vernetzung, nach der wir streben.

Ich möchte jetzt kurz auf die Vertraulichkeitscharta eingehen. Im Vereinigten Königreich haben wir im September 2001 zusammen mit dem Arbeitgeberverband

einen Bericht veröffentlicht, wonach gegenüber den Strafverfolgungsbehörden zwei Drittel der Sicherheitsverstöße nicht zur Anzeige gebracht wurden. Man hatte versucht, diese im eigenen Bereich zu bewältigen. Die Strafverfolgungsbehörden müssen verantwortlich die Rahmenbedingungen dafür schaffen, dass die Industrie mit den Strafverfolgungsbehörden zusammenarbeitet. Dies kann nur auf Basis gegenseitigen Vertrauens geschehen. Häufig fürchtet die Industrie, dass sich ein Schaden für die Marke oder das eigene Unternehmen einstellt. Das Wichtigste ist die wirtschaftliche Kontinuität, die zu berücksichtigen ist und die wir auch in unserem Kontaktprogramm ganz dick unterstrichen haben. Es ist immer noch sehr verbreitet, dass Unternehmen denken, die Polizei kommt mit einem großen Absperrband, macht alles für die Öffentlichkeit Sichtbare dicht und versucht dann alle beweiserheblichen Fakten in diesem abgesperrten Bereich zu sammeln. Dieses Bild schreckt die Industrie natürlich ab. Deshalb meinen Sie, sie müssten isoliert, abgeschottet von den Strafverfolgungsbehörden vorgehen. Aber das ist eine kurzsichtige, risikoreiche Vorgehensweise. Diese Vorgehensweise der Industrie wäre auf einer überholten Klischeevorstellung gegründet und hat mit der Vorgehensweise der Polizei im 21. Jahrhundert nichts mehr zu tun.

Wir haben uns beim Auflegen unserer neuen Strategie bereits einen neuen Ruf erworben. Wir haben uns auf die Bedürfnisse der Privatwirtschaft eingestellt und wir haben erkannt, dass wir gemeinsame Ziele verfolgen. Unser Bestreben ist es, einen gesetzeskonformen Marktplatz im Cyberspace zu schaffen. Einen Marktplatz frei von Kriminalität. Wir mussten Systeme entwickeln, die es uns gestatten, Erkenntnisse entsprechend zu sammeln und zu verarbeiten. Es gibt im kommerziellen Cyberspace sehr viele Geschäftsgeheimnisse und geistiges Eigentum. Deshalb bedurfte es eines Konzepts, um geschäftlich vertrauliche und technisch sensible Daten auch entsprechend zu verarbeiten. Ganz entscheidend ist, dass man sich früh zusammensetzt, früh Kontakt aufnimmt, was die Partnerschaft mit der Industrie angeht. Diese Policy ist in der Charta auch zum Ausdruck gebracht worden und basiert auf unseren Erfahrungen in der wahren Welt. Es kommt sehr häufig vor, dass uns Rechtsanwälte ansprechen und uns Szenarien schildern, die sie als hypothetisch darstellen. Wir erklären ihnen dann, wie wir in einem solchen Fall vorgehen würden. Und sobald wir ihnen erklärt haben, wie wir vorgehen würden und dass wir vertraulich vorgehen würden, berichten sie uns, dass eine tatsächliche Straftat dahintersteht. Das zeigt uns, dass das Hauptanliegen der Privatwirtschaft darin besteht, letzten Endes Kontrolle über das zu haben, was abläuft. Deshalb stellen wir aufgrund der Vereinbarungen in der Charta fachlich versiertes Personal bereit, das auch den Interessen der Industrie Rechnung trägt.

In unserer Tactical and Technical Support Section, also in unserem Taktischen und Technischen Unterstützungszentrum, haben wir Polizeibeamte, die aus verschiedenen Strafverfolgungsbehörden kommen und die darüber hinaus über Spezialkenntnisse in anderen Bereichen verfügen, beispielsweise den Einsatz technischer Mittel, verdeckte Polizeiarbeit oder Rechtshilfe. Das heißt, wir versuchen

für die Zusammenarbeit eine sichere Umgebung für die Unternehmen zu schaffen. Wenn man Erkenntnisse nur für Ermittlungszwecke weitergeben möchte, dann wird von uns Vertraulichkeit gewährleistet. Wir nutzen die üblichen Schutzmechanismen bei Quellen, die bisher von den Strafverfolgungsbehörden nur im Zusammenhang mit dem Einsatz von Informanten oder Vertrauenspersonen eingesetzt wurden. Die Auswertungsprodukte, die wir erstellen, werden nur in Zusammenarbeit und in Absprache mit dem Besitzer der Information geleistet; und nur mit dessen Zustimmung werden die Informationen weitergegeben. Es gibt jedoch eine einzige Ausnahme. Nämlich dann, wenn es um Menschenrechtsverletzungen geht, wenn es um die Verletzung wesentlicher Grundrechte geht. Dann sind wir natürlich gefordert einzuschreiten. Das ist ein Legalitätsanspruch, der besteht. Dann muss die Polizei natürlich handeln. Wenn es um das Leben einer Person geht, besteht für uns die Pflicht einzuschreiten. Das heißt noch nicht, dass auch tatsächlich ein förmliches Verfahren eingeleitet wird.

Wenn wir Informationen benötigen, um ein Verfahren beweisfest zu machen, dann arbeiten wir mit den Fachleuten für Risikomanagement in den Unternehmen zusammen. Wir versuchen alles, um eine Beeinträchtigung des Geschäftsbetriebes auf ein Minimum zu reduzieren. Hauptziel ist es, die Geschäftstätigkeit aufrechtzuerhalten. Wir haben einmal eine Person ermittelt, die wir festnehmen mussten. In Absprache mit dem Unternehmen haben wir uns darauf geeinigt, die Person am Wochenende festzunehmen, damit die Belegschaft nichts davon erfährt und so den Betriebsfrieden zu wahren. Das heißt, die Beziehung, die wir haben, muss zum beiderseitigen Vorteil gereichen. Wenn Informationen weitergegeben werden, stellt sich die Frage, was das Unternehmen im Gegenzug dafür bekommt. Wir versuchen, die gesamten Informationen zusammenzutragen und auszuwerten. Wir nutzen Informationen aus verschiedenen Branchen und können so auch der Industrie Informationen bereitstellen, zu denen sie anderweitig keinen Zugang hätte. Wir verfolgen Trends. Wir analysieren die Lage und versuchen, durch unsere Prognosen, durch unsere Lageanalysen, einen Mehrwert zu erzielen, von dem auch die Industrie profitiert. Das ist eine neue Dimension für das Risk Management auf Seiten der Industrie. Natürlich fließen unsere Erkenntnisse auch in die Risikobewertung der Unternehmen ein. Und wir können sie dabei beraten, wie sie eine bestmögliche Risikoanalyse und ein Risikomanagement durchführen.

Natürlich ist eine Schlüsselaufgabe von uns die Verfolgung und Festnahme von Straftätern. Deshalb geht es darum, ein Forum einzurichten, in dem wir uns mit unseren Partnern austauschen können. Ich bin auch stolz darauf, dass wir von der Industrie für die Schnelligkeit, mit der wir reagieren können, gelobt wurden. Viele sind überrascht, dass wir mit unseren ausländischen Partnerdienststellen, falls erforderlich, innerhalb von Stunden vor Ort im Einsatz sein können.

Wir glauben, dass wir das Problem schon ganz gut im Griff haben. Aber wir behaupten nicht, dass wir es schon vollständig in all seinen Facetten verstehen. Wir

wissen, dass es Unternehmen gibt, die glauben, dass sie die Situation vollständig im Griff haben, alle Systeme bereits eingesetzt haben. Für uns ist es wichtig zu wissen, wo wir einen Mehrwert einbringen können. Es gibt sehr viele internationale Organisationen, Unternehmen, die in der Lage sind, Informationen schnell beizuziehen, zu steuern – weltweit. Mit denen sollten wir nicht konkurrieren. Aber wir sollten in der Lage sein zu sagen, was gemacht werden kann, wenn die Informationstechnologie einmal nicht mehr so funktioniert, wie wir es uns vorstellen. Das ist meines Erachtens der Anteil, den wir in die Partnerschaft einbringen sollten.

Kritische Infrastrukturen: Präventionsmaßnahmen aus Sicht des BSI

Udo Helmbrecht

Sehr geehrte Damen und Herren,

rund drei Monate ist es jetzt her, als der letzte große Computerwurm durchs Internet schwirrte. Wahrscheinlich denken viele von Ihnen noch mit Schrecken an „Blaster" – auch „Lovsan" genannt – zurück. Millionen Nutzer des Betriebssystems Windows waren weltweit außer Gefecht gesetzt – gleichzeitig wurden Ihre Rechner für einen Angriff auf Microsoft missbraucht. Besonders schlimm war, dass sich „Blaster" – im Gegensatz zu herkömmlichen Computerschädlingen – nicht per E-Mail verbreitete, sondern die Rechner direkt über das Internet angegriffen hat. Eine lange vorher bekannt gewordene Sicherheitslücke öffnete dem Schädling die Türen zu Millionen PCs. Betroffen waren vorwiegend Privatanwender. Was aber wäre, wenn ein solcher Computerschädling alle IT-Systeme lahm legen würde? Sind wir auf eine solche Attacke wirklich vorbereitet?

Nun, meine Damen und Herren, diese Frage kann ich Ihnen mit einem einfachen „Nein" beantworten. Aber: Inzwischen steuern Computer unsere Energiesysteme. Sie lenken Verkehrs- und Informationsströme. Computer machen den modernen Zahlungsverkehr erst möglich. Wenn also die Computer nicht mehr funktionieren, dann kann auch der Staat und die Gesellschaft nicht mehr reibungslos funktionieren. Denn dafür müssen die notwendigen Infrastrukturen störungsfrei verfügbar sein. Solche Infrastrukturen nennen wir Kritische Infrastrukturen. Das sind in Summe alle Organisationen und Einrichtungen, die für das staatliche Gemeinwesen von lebenswichtiger Bedeutung sind. Dabei reden wir über die Informations- und Kommunikationstechnik, den Energiesektor, das Finanz- und Versicherungswesen, den Transport- und Versorgungssektor, das Notfall- und Rettungswesen genauso wie über das Gesundheitswesen und schlussendlich natürlich auch über die Verwaltung.

Mit der zunehmenden IT-Durchdringung sind unsere Infrastrukturbereiche auch durch die Informationstechnik verwundbar geworden. Gezielte Angriffe von außen können massive Störungen hervorrufen. Störungen oder Ausfälle können wir uns aber nicht leisten. Sie würden für große Bevölkerungsgruppen zu nachhaltig wirkenden Versorgungsengpässen führen. Oder sie könnten andere dramatische Folgen haben. Bei besonders IT-abhängigen Prozessen sind durch Kettenreaktionen auch Störungen in anderen Bereichen möglich. Auswirkungen auf die innere Sicherheit und in einigen Fällen sogar die äußere Sicherheit Deutschlands könnten die Folge sein.

Das Bundesamt für Sicherheit in der Informationstechnik beschäftigt sich daher mit der Frage, ob und wie durch Eingriffe über die Informationstechnik unsere Volkswirtschaft massiv geschädigt und wie die innere Sicherheit beeinträchtigt

werden kann. Wir schauen dabei eher auf den technischen Ansatz. Kurz gesagt: Uns interessiert nicht, wer uns den Strom abstellt, sondern ob es jemand tun könnte. Und wenn ja, wie er es macht – und was wir dagegen tun können.

Der neue Präsident des BSI, Dr. Udo Helmbrecht

Meine sehr geehrten Damen und Herren,

jeder geht täglich mit Informations- und Kommunikationstechnik um – häufig ohne es zu bemerken. So selbstverständlich ist es geworden. Informationstechnik ist der ständige Begleiter des modernen Lebens. Ohne sie ist unser – westlich zivilisiertes – Leben kaum mehr vorstellbar. Kurz gesagt: Wir sind abhängig. Wir sind abhängig vom Funktionieren kritischer Infrastrukturbereiche. Denn würden diese versagen, dann würde wahrscheinlich nicht nur das wirtschaftliche und gesellschaftliche Leben in Deutschland zum Erliegen kommen. Es würden auch andere Länder in Mitleidenschaft gezogen werden.

Ein Beispiel dafür – wenn auch ohne direkten Bezug zur Informationstechnik – ist der Stromausfall im September in Italien. 57 Millionen Menschen saßen im Dunkeln. Zum Glück war es Sonntag Nacht. Das ganz große Chaos blieb deshalb aus. Aber: Dieses Beispiel macht deutlich, wie groß die Vernetzung inzwischen ist. Denn Italien ist auf Stromimporte aus Frankreich, der Schweiz und Österreich angewiesen. Nach den letzten Erkenntnissen war lediglich ein umgestürzter Baum

der Grund für den Stromausfall in Italien. Ein Übergreifen auf Deutschland konnte durch schnelle Gegenmaßnahmen verhindert werden.

Von diesen Beispielen könnte ich Ihnen noch unzählige mehr aufzählen, das Ergebnis wäre immer das gleiche: Wir sind abhängig. Bisher gab es zwar noch keine Katastrophe, bei der eine Störung einen Totalausfall aller Kritischen Infrastrukturen verursachte. Dennoch: Wo wir können, müssen wir vorsorgen und uns schützen!

Als BSI ist es unsere Aufgabe, für den Schutz der Informationstechnik zu sorgen. Wir weisen auf Abhängigkeiten hin und versuchen diese zu minimieren. Konkret heißt das: Wir schlagen technische und organisatorische Maßnahmen vor, die helfen sollen, Störungen oder Ausfälle der Informationstechnik zu vermeiden. Oder wir kümmern uns – wenn die Störungen nicht vermeidbar sind – um geeignete Mittel, sie zu beheben. Alles unter der Maßgabe, dass die Störungen auf Fehlfunktionen oder auf Ausfälle der Informationstechnik zurückzuführen sind – egal ob absichtlich herbeigeführt oder versehentlich.

Das BSI hat vor über zwei Jahren damit begonnen, die Kritischen IT-Infrastrukturen genauer zu untersuchen. Vor einigen Jahren sah es folgendermaßen aus: Viele Sektoren waren nur regional organisiert. Eine überregionale Vernetzung war kaum vorhanden. Die Funktionsfähigkeit der Infrastrukturen konnte dadurch nur lokal beeinträchtigt werden.

Heute sieht die Situation anders aus: Die Sektoren sind immer stärker auch untereinander vernetzt. Das Bindeglied zwischen allen Wirtschaftsbereichen ist die Informationstechnik. Deshalb geht es beim Schutz der Kritischen Infrastrukturen in aller erster Linie auch um den Schutz der Informationstechnik.

Das Konzept „Schutz Kritischer Infrastrukturen“ unterscheidet sich besonders in einem Punkt von der rein technischen IT-Sicherheit: Es berücksichtigt auch gesamtgesellschaftliche Risiken und bindet sie staatenübergreifend in ein allgemeines Sicherheitsverständnis ein. Die Ergebnisse unserer Untersuchung sind insgesamt unterschiedlich ausgefallen: Viele kritische Bereiche sind ausreichend geschützt, in anderen besteht Handlungsbedarf, auch wenn es aktuell zum Glück nirgendwo „brennt“.

Meine Damen und Herren,

nicht nur durch den flächendeckenden Einsatz der Informationstechnik sind wir abhängiger geworden. Auch durch die komplexen Zusammenhänge und das Zusammenspiel der Infrastrukturbereiche steigt das Risiko, dass es zu Störungen kommen kann. Die Effizienzsteigerung, die zunehmende Internationalisierung, der Abbau von Überkapazitäten – all das fordert seinen Tribut.

Ein Angreifer hat hier immer leichteres Spiel. Das Internet stellt potenziellen Angreifern das notwendige Wissen kostenlos zur Verfügung. Angreifer haben genügend Vorbereitungszeit, sie müssen – anders als bei Terroranschlägen – nicht

einmal direkt vor Ort sein, um den Schaden zu verursachen. Angriffe können automatisiert und vor allem gleichzeitig durchgeführt werden. Dadurch ist die Geschwindigkeit und Wirksamkeit der Durchführung enorm hoch. Zudem kann der Angriff aus sicherer Umgebung gestartet werden, zum Beispiel von einer Insel aus, die kein Rechtshilfeabkommen mit Deutschland hat. Eine Strafverfolgung ist dann kaum möglich. Eine potenzielle Tätergruppe für derartige Angriffe sind Terroristen. Aber mindestens genauso ernst nehmen müssen wir Wirtschaftskriminelle, Hacktivisten, Script-Kiddies, Spione und die so genannten Innentäter.

Aber wo liegen unsere größten Schwachstellen? Hier gibt es eine Reihe an Defiziten: Angefangen bei fehlenden strategischen IT-Sicherheitsbetrachtungen und Managementvorgaben, über die zunehmende Vernetzung, unregelmäßige Updates, bis hin zu schlichter Bequemlichkeit. Die Achillessehne ist das vielerorts mangelnde Sicherheitsbewusstsein. Zudem kann unzureichend ausgebildetes Personal genauso problematisch sein wie die Auslagerung von kritischen Geschäftsbereichen, aus denen sich per se eine starke Abhängigkeit ergibt. Aber: Wer sich keine Reserven mehr leisten kann und will, muss im Krisenfall mit den Folgen leben.

Stichwort Krisenfall. Was müssen wir schützen? Natürlich all das, woran uns etwas liegt – nämlich das Leben, die Gesundheit sowie Sach- und Vermögenswerte. Aber auch das Vertrauen der Bürger in das Gemeinwesen zu schützen ist wichtig. Verlieren wir dieses Vertrauen oder wird es durch Ausfälle Kritischer Infrastrukturen geschädigt, sind volkswirtschaftliche Schäden kaum abzuwenden. Generell ist es das Ziel, den Schaden zu begrenzen. Konkret heißt das: Wenn überhaupt, dann soll ein Schaden nur selten auftreten. Und dann auch nur kurz. Die Schäden sollen möglichst geringe Auswirkungen haben, beherrschbar, isolierbar und reparabel sein.

Inzwischen sind die IT-Systeme jedoch so komplex geworden, dass de facto gar kein Täter mehr notwendig ist, um einen Schaden anzurichten. Die Systeme fallen auch von allein aus. Man möchte gar nicht darüber nachdenken, was passiert, wenn dann noch intelligente Täter am Werk sind.

Meine sehr geehrten Damen und Herren,

ich gebe zu: Die Verantwortlichen haben es nicht leicht. Schnelle Innovationszyklen, komplexe Programme, der Mangel an Fachkräften – das sind nur ein paar Problemfelder. Aber wer ist denn überhaupt für den Schutz der Kritischen Infrastrukturen verantwortlich? Fest steht: Für diesen Schutz kann niemand allein verantwortlich sein. Zum einen ist es natürlich Aufgabe des Staates für die Sicherheit der Kritischen Infrastrukturen zu sorgen. Das geht aber nur Hand in Hand mit der Wirtschaft. Keiner kann autonom handeln. Schließlich ist ein Großteil der Infrastrukturen in der Verantwortung der Wirtschaft. Selbst ehemals staatliche Domänen sind zunehmend privatisiert – wie die Deutsche Telekom, die Deutsche

Post oder auch die Deutsche Bahn. Deshalb ist auch die Eigenverantwortung der Wirtschaft und der privaten Nutzer gefordert.

Vorsorge statt Nachsorge – lautet das Motto. Die zahlreichen Computerwürmer in diesem Jahr haben das deutlich gemacht. Wir können von Glück reden, dass die meisten Ausfälle am Wochenende stattfanden, so blieben uns größere Schäden erspart. Deutlich wird jedoch: reaktive Maßnahmen reichen keinesfalls aus. Und damit komme ich zum Stichwort Prävention.

Zuerst das Erfreuliche: Sie können Ihre IT-Infrastruktur schützen. Prävention ist jedoch vor dem Eintritt eines Schadens erforderlich. Wer ins Wasser fällt und nicht schwimmen kann, der kann es dann auch nicht mehr lernen. Schauen Sie sich also die IT-Infrastruktur in Ihrem Unternehmens- oder Behördenumfeld an. Entscheiden Sie, an welcher Stelle die Informationstechnik für Sie unverzichtbar funktionsfähig sein muss. Ergreifen Sie angemessene Schutzvorkehrungen für die Sicherheit Ihrer Informationstechnik und damit Ihres Unternehmens. Fast immer ist es möglich, mit relativ geringem Aufwand die Sicherheit im Vorfeld deutlich zu verbessern. Und das ist natürlich immer günstiger als bis zum Eintritt eines Schadens zu warten.

Es gibt aber auch eine schlechte Nachricht: Nichtsdestotrotz können wir die Informationstechnik nicht für jeden denkbaren Fall ausreichend schützen. Es kann Situationen geben, in denen ein normalerweise ausreichender Schutz nichts nützt. Aber auch für diesen Fall sollten Sie sich die Fragen stellen: Was mache ich dann? Gibt es einen Notfall- und Alarmierungsplan? Sonstige Krisenpläne? Werden zum Beispiel die Daten regelmäßig gesichert?

Die Erfahrungen des BSI haben gezeigt, dass gerade die Prävention im Bereich der Behörden und der Verwaltung nicht überall ausreichend ist: Kontrollmechanismen zur IT-Sicherheit wurden bislang nicht ausreichend implementiert. An allen Ecken und Kanten fehlt qualifiziertes Fachpersonal. Den Mitarbeitern und Entscheidern mangelt es oft an einem ausreichenden Sicherheitsbewusstsein. Notfallkonzepte und Notstromversorgungen sind nur selten verfügbar. Es gibt also genügend Sicherheitslücken.

Und selbst wer über Vorsorgekonzepte verfügt, darf sich nicht in falscher Sicherheit wiegen. Diese nützen nämlich nichts, wenn sie in der Schublade liegen. Sie müssen umgesetzt werden. Das gilt für alle Arbeitsprozesse, aber besonders auch für die Informationstechnik. Daten können schnell verloren gehen. Deshalb ist der Schutz von Kritischen Infrastrukturen in erster Linie auch das ureigene Interesse und Verantwortlichkeit der Betreiber.

Meine Damen und Herren,

der Schutz, über den wir hier sprechen, geht über die normalen IT-Sicherheitsmaßnahmen hinaus. Die Standardschutzmaßnahmen sind quasi das Basislager der Bergbesteigung. Für den Aufstieg zum Gipfel müssen Sie weitere Maßnah-

men ergreifen. Aber kaum jemand kann sich IT-Sicherheit nach dem Gießkannenprinzip leisten. Man muss gezielt vorgehen – sowohl aus Kosten- als auch aus Effektivitätsgründen.

Deshalb empfiehlt das BSI folgende Maßnahmen um den Schutz der Kritischen Infrastruktur zu gewährleisten:

Der Schutz dieser Infrastrukturen ist wegen der weitreichenden Konsequenzen Managementaufgabe. Was uns dabei aber immer wieder wundert, ist, dass das Management normalerweise zwar systematisch vorgeht. Bei der IT-Sicherheit können wir Systematik und Konsequenz aber oft nicht erkennen. Hier kommt meist nur das Feuerlöscherprinzip zur Anwendung. Ein Backup hier, eine Sicherheitsrichtlinie dort. Die Herstellung und Verbesserung der Sicherheit erfordern allerdings ein systematisches Vorgehen. Dabei müssen Zusammenhänge und Abhängigkeiten erkannt und – noch wichtiger – berücksichtigt werden. Das heißt konkret, dass Abhängigkeiten reduziert werden müssen und unabhängige, autarke Arbeitsmodule angestrebt werden sollten. Wichtig sind die bereits angesprochenen Redundanzen für identifizierte kritische Systeme sowie Notfallpläne und Krisenkonzepte. Bei denen sollte die Probe aufs Exempel aber schon vor der Krise stattfinden. Dafür sind entsprechende Ressourcen in Form von Geld, Zeit und Personal notwendig.

In vielen Organisationen wird zudem der Faktor Mensch oft vergessen. Der Mensch gilt noch immer als größtes Risiko. Und hierbei vor allem die Innentäter: Zwei von drei Angriffen stammen von den eigenen Mitarbeitern! Mitarbeiter, IT-Fachkräfte und auch die Führungskräfte müssen sensibilisiert werden.

Und schließlich ist auch klar: Sicherheit kann nur durch die Kombination aus IT-Sicherheit und physikalischer Sicherheit, z. B. durch Zugangskontrollen, erreicht werden.

Sehr geehrte Damen und Herren,

das BSI ist verantwortlich für IT-Sicherheit in Deutschland – und damit sind wir auch in der Verantwortung, den Schutz der Kritischen Infrastrukturen zu unterstützen.

Das Bundesministerium des Innern arbeitet derzeit an einem „Nationalen Plan zum Schutz der IT-abhängigen Kritischen Infrastrukturen“. Das BSI ist daran maßgeblich beteiligt. Ich gehe davon aus, dass die Konzeption, wie der Schutz der Kritischen Infrastrukturen in den nächsten Jahren gestaltet werden soll, bis Ende 2004 steht. Der Schwerpunkt wird ganz klar auf der Prävention liegen, um einen national angemessenen und ausgewogenen Infrastrukturschutz zu erhalten. Der verantwortungsbewusste und angemessene Umgang mit Vorfällen steht aber ebenfalls auf der Agenda.

Darüber hinaus denken wir an Kooperationen. Mögliche Partner sind für uns das Bundeskriminalamt sowie das gerade in seiner Entstehung befindliche Bundes-

amt für Bevölkerungsschutz und Katastrophenhilfe. Zwischen Wirtschaft und Staat existieren bereits intensive KRITIS-Kooperationen. Unter dem Stichwort „Kooperation KRITIS“ bietet das BSI eine Kommunikationsplattform für IT-spezifische Probleme von Wirtschaftsunternehmen im Bereich Kritischer Infrastrukturen an. Wichtig ist hier der vertrauensvolle Informationsaustausch.

In Kürze bieten wir zusätzlich einen Fragebogen zur schnellen Identifikation Ihrer kritischen IT-Prozesse. Der Fragebogen berücksichtigt einerseits die Einschätzung des Managements hinsichtlich der Kritikalität der Geschäftsprozesse. Andererseits kommt die Einschätzung der IT-Leitung in Bezug auf die Kritikalität der unterstützenden IT-Anwendung nicht zu kurz.

Nicht vergessen möchte ich auch unsere übrigen Dienstleistungsangebote, die keinen unmittelbaren Bezug zum Schutz der Kritischen Infrastrukturen haben, dafür aber unabdingbar sind. Dazu zählen CERT-Bund sowie das IT-Penetrationszentrum. Beide beschäftigen sich mit Angriffen über das Internet, die eine akute Gefahr für alle Computernetzwerke sind. CERT Bund könnte man als Spezialeinheit für Netzwerksicherheit bezeichnen. Vor allem nach Angriffen auf IT-Systeme kommt CERT Bund auf den Plan. Ziel ist es Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computer-Systemen bereitzustellen – an einer zentralen Anlaufstelle. Und das sowohl präventiv als auch reaktiv. Diese Dienstleistung steht in erster Linie den Bundesbehörden in Form einer 24-Stunden-Rufbereitschaft und dem Betrieb eines Lagezentrums zur Verfügung. Auch für Unternehmen gibt es am Markt bereits CERTs. Eines davon – und speziell für den Mittelstand – wird ab Mitte Dezember Mcert sein. Der federführende Betreiber von Mcert wird BITKOM in Kooperation mit dem Innenministerium, anderen Partnern und uns sein.

Das IT-Penetrationszentrum kommt – anders als CERT Bund – vor einem Angriff zum Zug. Mit Penetrationstests überprüfen wir die Sicherheit von IT-Systemen. Oft finden wir dabei ungeahnte Sicherheitslücken in den Abwehr- und Schutzsystemen.

An dieser Stelle möchte ich auch auf unsere Empfehlungen für den Bereich IT-Grundschutz hinweisen. Viele von Ihnen kennen sicher das IT-Grundschutzhandbuch – mit über 2.000 Seite das Standardwerk der IT-Sicherheit.

Eine Hilfestellung zur verbesserten IT-Sicherheit – gerade auch bei kritischen Prozessabläufen – ist darüber hinaus die IT-Sicherheitszertifizierung. Der Einsatz von Produkten, die auf Ihre Sicherheit geprüft wurden, trägt ebenso wie eine zertifizierte IT-Ablauforganisation zu Ihrer Sicherheit bei. Speziell für Bundesbehörden bieten wir auch eine IT-Sicherheitsberatung an.

Unsere Grundlagenforschung im Bereich Internetsicherheit und Kryptologie sowie die Maßnahmen zur Lauschabwehr gehören ebenfalls zu unseren Aufgaben.

Meine sehr geehrten Damen und Herren,
IT-Sicherheit ist Managementaufgabe. Die Verantwortung liegt bei den Führungskräften und (in Behörden) bei der Hausleitung. Bereits bei der Haushaltsaufstellung sollte darauf geachtet werden, dass später ausreichend Mittel zur Verfügung stehen, damit notwendige Vorkehrungen getroffen werden können.

Das Ziel ist eine durchgängige IT-Sicherheitspolitik. Zugegeben: Sie müssen dafür eine ganze Reihe an Maßnahmen umsetzen. Sie müssen die Risiken organisationsübergreifend betrachten und lokal analysieren und IT-Sicherheitsleitlinien einführen. Skalierte IT-Sicherheitsvorgaben sind ein weiteres Muss. Aber die Mühe lohnt sich: Das Ergebnis ist ein angemessener und wirtschaftlich vertretbarer IT-Schutz. Zwar gibt es im Bereich der Kritischen Infrastrukturen derzeit keine akuten IT-Verwundbarkeiten, aber dennoch müssen wir schon jetzt handeln. In Zukunft werden die IT-Gefährdungen durch die IT-Durchdringung weiter zunehmen. Spätestens dann kommen alle Beteiligten in Zugzwang.

E-Commerce, eine erste Bewertung

Helke Heidemann-Peuser

Sehr geehrter Herr Präsident,
sehr geehrte Damen und Herren,

im Auftrag von Frau Professor Müller möchte ich dem Bundeskriminalamt herzlich für die Einladung zu dieser Veranstaltung danken. Sie gibt uns Gelegenheit, zu dem wichtigen Thema E-Commerce aus Verbrauchersicht anhand der Erfahrungen aus den letzten Jahren Stellung zu nehmen.

Gestatten Sie mir, bevor ich auf das Thema eingehe, den Verbraucherzentrale Bundesverband und die Organisation der Verbraucherarbeit in Deutschland kurz vorzustellen:

Der Verbraucherzentrale Bundesverband[1] ist das Ergebnis einer Strukturreform der Verbraucherarbeit in Deutschland aus dem Jahre 2000, durch die drei Bundesorganisationen, nämlich die Arbeitsgemeinschaft der Verbraucherverbände e. V., der Verbraucherschutzverein e. V. und die Stiftung Verbraucherinstitut zu einem Bundesverband zusammen geschlossen wurden.

Der vzbv ist die bundesweite Dachorganisation der 16 Verbraucherzentralen und 23 weiterer sozial orientierter Verbände, wie etwa dem Deutschen Hausfrauenbund oder der Arbeiterwohlfahrt. Finanziert wird seine Arbeit größtenteils aus Mitteln des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft. Im Jahre 2002 betrug die Zuwendung 7,7 Millionen Euro. Hinzu kamen Einnahmen aus dem Verkauf von Publikationen sowie Projektmittel in Höhe von ca. 900.000 Euro. Der Gesamtetat betrug 8,6 Millionen Euro.[2] Der vzbv verfügt über 72 Planstellen. Der Sitz des Verbandes ist in Berlin.

Zu den Aufgaben des Verbraucherzentrale Bundesverbandes gehören insbesondere die Interessenvertretung der Verbraucher in der Öffentlichkeit und gegenüber Politik, Wirtschaft und Zivilgesellschaft, ferner die berufliche Qualifikation in der Verbraucherarbeit durch Schulungsmaßnahmen für Multiplikatoren sowie die Wahrnehmung der Verbandsklagebefugnis nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) und dem Unterlassungsklagengesetz (UKlaG). Auf dieses Klagerecht werde ich später noch näher eingehen.

Der vzbv ist aktives Mitglied des europäischen Verbraucherverbandes BEUC[3] und als Mitglied im Rat von Consumers International (CI)[4] vertreten, dem Weltverband der Verbraucherorganisationen.

---

1 www.vzbv.de
2 Vgl. vzbv-Jahresbericht 2002/2003, S. 83.
3 www.beuc.org
4 www.consumersinternational.org

Mit Helke Heidemann-Peuser war erstmals eine Vertreterin der Verbraucherzentralen zu Gast im BKA

Wirtschaftliche Bedeutung des E-Commerce

Durch den elektronischen Handel wurde in den letzten Jahren für Verbraucher eine völlig neue Einkaufsmöglichkeit eröffnet. Das Internet erlaubt – außerhalb jeglicher Ladenöffnungszeiten – den Zugang zu Dienstleistungs- und Warenangeboten weltweit. Bis dahin nicht bekannte Vertriebsformen, wie etwa die Internet-Auktion, sind entstanden. Bankgeschäfte können von zu Hause aus erledigt, ebenso können Reisen vom eigenen PC aus verbindlich gebucht werden.

Das Marktforschungsunternehmen Forrester Research schätzt laut einer Veröffentlichung in der FAZ vom 17. 11. 2003[5], dass Europas Verbraucher in diesem Jahr 9 Milliarden Euro für Weihnachtsgeschenke im Internet ausgeben, 2,5 Milliarden allein in Deutschland. Besonders gefragt sind danach Billigreisen und Bücher, aber auch in den Bereichen Technik, Schmuck und Mode hofft der Versandhandel auf hohe Umsätze. In den USA werden für Weihnachten sogar Umsätze i. H. von 12 Milliarden Dollar erwartet. Diese Zahlen belegen, welchen Stellenwert der Wirtschaftsfaktor E-Commerce inzwischen weltweit erreicht hat. Mit der wachsenden Zahl der Internetanschlüsse in den privaten Haushalten wird dieser Markt weiter an Bedeutung gewinnen.

5 Frankfurter Allgemeine Zeitung v. 17. 11. 2003, Nr. 267, S. 19.

Andererseits schrecken nach wie vor viele Verbraucher insbesondere vor grenzüberschreitenden Geschäftsabschlüssen im Internet zurück. Die Gründe sind mangelndes Vertrauen in das Gelingen der Transaktion, zum Teil begründet durch eigene schlechte Erfahrungen, Unsicherheit über das anzuwendende Recht und die Möglichkeiten der Rechtsdurchsetzung. Nachfolgend möchte ich daher einen kurzen Überblick über die rechtlichen Grundlagen für den elektronischen Handel in Deutschland geben.

Gesetzliche Grundlagen

– Der europäische Gesetzgeber hat durch die Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr vom 8. Juni 2000 (E-Commerce-Richtlinie)[6] einen gemeinsamen Rechtsrahmen für den elektronischen Geschäftsverkehr in der Europäischen Union geschaffen. Sie regelt sowohl den Geschäftsverkehr zwischen den Unternehmen (B2B) als auch zwischen Unternehmen und Verbrauchern (B2C). Ziel ist es u. a., durch einen effektiven Schutz der Verbraucher die Akzeptanz des elektronischen Geschäftsverkehrs zu stärken und Markttransparenz zu schaffen. Die Richtlinie dient auch der Förderung des freien Waren- und Dienstleistungsverkehrs. Sie regelt u. a. Informationspflichten des Unternehmers sowie Modalitäten des Vertragsabschlusses. Diese Vorschriften wurden in Deutschland durch das Schuldrechtsmodernisierungsgesetz mit Wirkung vom 2. Januar 2002 umgesetzt (§ 312 e BGB).

– Ferner gelten für Vertragsabschlüsse unter Verwendung von Fernkommunikationsmitteln die Vorschriften der Fernabsatzrichtlinie aus dem Jahr 1997, bei uns umgesetzt durch das seit dem 30. 6. 2000 geltende Fernabsatzgesetz, das durch die Schuldrechtsmodernisierung in das BGB (§§ 312b-d) integriert wurde.

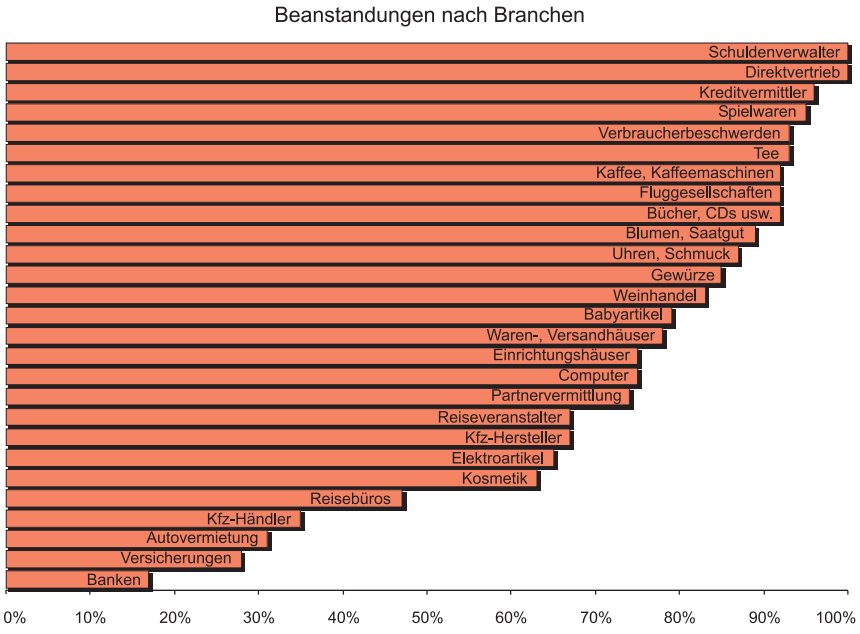
– Zu erwähnen ist darüber hinaus das ebenfalls der Umsetzung der E-Commerce-Richtlinie dienende Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (EGG) vom 14. 12. 2001[7], das zu Änderungen im Teledienstegesetz und Teledienstedatenschutzgesetz (TDDSG) geführt hat. Mit dem EGG wurde außer bei Verträgen mit Verbrauchern das Herkunftslandprinzip eingeführt wurde. Für Verbraucherverträge bleibt Artikel 29 EGBGB maßgebend. Das heißt, bei Verbraucherverträgen gilt grundsätzlich das Recht des Staates, in dem der Verbraucher seinen gewöhnlichen Aufenthaltsort hat. Zwar ist eine vertragliche Rechtswahl grundsätzlich möglich. Dem Verbraucher darf dadurch jedoch nicht der Schutz entzogen werden, der ihm durch zwingende Vorschriften in dem Mitgliedstaat gewährt wird, in dem er seinen Wohnsitz hat.

6 Amtsblatt EG Nr. L 178 v. 17. 7. 2000, S. 1–16.
7 BGBl 2001 Teil I Nr. 70 v. 20. 12. 2001, S. 3721.

– Der Gerichtsstand bestimmt sich nach der Gerichtsstand- und Vollstreckungsverordnung (EuGVO Nr. 44/2001)[8]. Danach kann der Verbraucher im Falle einer von ihm angestrengten Klage den Gerichtsstand wählen, der Unternehmer dagegen ist gezwungen, am Wohnsitz des Verbrauchers seine Klage zu erheben.

Mängel beim Internetauftritt

Nach Erfahrungen der Verbraucherverbände werden die gesetzlichen Informationspflichten nicht in ausreichendem Maße beachtet. Das ist das Ergebnis einer Untersuchung von über 500 Internetangeboten, die der Verbraucherzentrale Bundesverband e. V. im Zeitraum Oktober 2002 bis Februar 2003 durchgeführt hat. 71 % der Internetangebote, also nahezu drei Viertel, verstießen gegen die gesetzlichen Vorschriften; lediglich 29 % der Anbieter waren nicht zu beanstanden. Die Verstöße ziehen sich quer durch alle Branchen:



– Verstöße gegen § 6 Teledienstegesetz

Es wurden 447 Verstöße gegen die Anbieterkennzeichnungspflicht aus § 6 TDG festgestellt.

8 Amtsblatt EG 2001, Nr. L 12, S. 1.

Die weitaus häufigsten Zuwiderhandlungen betrafen fehlende oder ungenügende Angaben zu Namen, Niederlassungsanschrift und – bei Gesellschaften – zu Vertretungsberechtigten des Diensteanbieters. Als Name des Diensteanbieters wurde von Gewerbetreibenden häufig lediglich eine Geschäftsbezeichnung, bisweilen auch nur der Domainname genannt; zum Teil fand sich zwar der Nachname des Diensteanbieters, jedoch ohne oder nur mit abgekürzter Angabe des Vornamens. Statt der Niederlassungsanschrift war häufig nur eine Postfachangabe aufzufinden, bei Gesellschaften fehlte die Angabe eines Vertretungsberechtigten bzw. war nur eine presserechtliche Verantwortlichkeit benannt.

– Fernabsatzinformatonen

In 267 Fällen waren die bei Anbahnung eines Fernabsatzvertrags gem. § 312 c BGB i. V. m. § 1 BGB-Informationspflichten-Verordnung (BGB-InfoV) zu erteilenden Informationen unvollständig. Am auffälligsten waren folgende Verstöße:

Frappierend war die Anzahl der Verstöße gegen die Pflicht zur Information über die Art und Weise des Vertragsschlusses, wie sie in § 1 Abs. 1 Nr. 3 BGB-InfoV genannt sind. Die Vorschrift ist unter verbraucherschützenden Gesichtspunkten von erheblichem Belang. Denn die Information über die Art und Weise des Zustandekommens des Vertrags verdeutlicht dem Verbraucher zum einen seine Bindungsfrist an die eigene Bestellung, des weiteren definiert sie den Zeitpunkt des Entstehens vertraglicher Erfüllungsansprüche und ist schließlich auch Ausgangspunkt für den Beginn der vom Unternehmer vorbehaltenen Lieferfrist. Verstöße gegen diese Informationspflicht ziehen sich quer über alle Branchen.

Fehlende Hinweise auf das zweiwöchige Widerrufsrecht des Verbrauchers wurden ebenfalls gehäuft festgestellt. Auffällig war die Häufung der Verstöße bei Gewürz-, Tee- und Weinhändlern, was jedoch von der Fehlvorstellung einer generellen Ausnahme von Lebensmitteln vom Widerrufsrecht geleitet sein kann. Bei den restlichen Branchen entfielen etwa 20 % aller festgestellten Verstöße gegen Informationspflichten im Fernabsatz auf einen gänzlich fehlenden Hinweis zum Widerrufsrecht.

Bei Fernabsatzangeboten sind gem. § 312 c BGB die Informationsinhalte rechtzeitig vor Vertragsschluss sowie klar und verständlich zu erteilen. Fehlende Rechtzeitigkeit der Information war gegeben, wenn diese in Allgemeinen Geschäftsbedingungen enthalten war und im Verlauf des Bestellvorgangs kein Hinweis hierauf erfolgte.

– E-Commerce-Informationen

Online-shops verstießen in 320 Fällen gegen die im elektronischen Geschäftsverkehr einzuhaltenden Informationspflichten, die sich aus § 312 e BGB i. V. m. § 3 BGB-InfoV ergeben.

Oftmals erfolgte keine Information über die zum Vertragsschluss führenden Schritte. Bedenklich an diesem Ergebnis war die Vielzahl der Angebote, in denen jegliche Information über den Zeitpunkt der Bestellabgabe fehlte, der Bestellvorgang lediglich über mit der Bezeichnung „Weiter" beschriftete Schaltflächen geleitet wurde und auch die letzte, die Bestellung auslösende Schaltfläche nicht gesondert gekennzeichnet war. Der Kunde sendet bei diesen Angeboten also mangels klarer Information eine Bestellung, ohne in diesem Augenblick den Willen zu deren Abgabe zu besitzen.

Die mit Abstand am häufigsten durch die Anbieterseite vernachlässigte Information betraf Angaben darüber, ob der Vertragstext nach Vertragsschluss gespeichert wird und dem Kunden zugänglich ist. In der Regel fehlte sogar ein Hinweis darauf, zumindest die Bestellung in ihrem Wortlaut ausdrucken zu können oder die Information, eine Bestell- oder Auftragsbestätigung zu erhalten. In diesen Fällen war dem Kunden überhaupt keine Möglichkeit aufgezeigt, zumindest den Inhalt seiner Bestellung in dauerhaft wiedergabefähiger Form speichern zu können.

Bewertung

Die Mehrzahl der Verstöße dürfte auf mangelnde Kenntnis der Anbieterseite über die einzuhaltenden Rechtsvorschriften zurückzuführen sein. Diese Schlussfolgerung wird durch die erhebliche Anzahl der unternehmerseits zügig und vorbehaltlos erteilten Unterlassungserklärungen gerechtfertigt. Die Anbieterschaft ist also gewillt und bestrebt, gesetzliche Vorgaben einzuhalten.

Innerhalb der Unternehmerschaft besteht allerdings auch erhebliche Unsicherheit über die Auslegung der jeweiligen Vorschriften, was möglicherweise zum einen auf deren fehlende, rechtlich fundierte Beratung zurückgeführt werden kann, andererseits naturgemäß in der jungen Gesetzesmaterie selbst begründet ist, zu der bislang nahezu keine Leitlinien vorgebende obergerichtliche Rechtsprechung vorliegt.

Umsetzung der Untersuchungsergebnisse

Von den 357 beanstandeten Internetangeboten wurden 339 Anbieter wegen Verstoßes gegen § 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG) bzw. gegen § 2 Unterlassungsklagengesetz (UklaG) abgemahnt. Die geringfügige Differenz zwischen der Zahl der Beanstandungen und den Abmahnungen erklärt sich zum einen aus einer Reihe zwar deutschsprachiger, aber aus dem außereuropäischen Ausland betriebener Angebote, des weiteren aus letztendlich als dubios einzustufender Internetpräsenzen, bei denen sich eine Anbieterkennzeichnung weder auf der Homepage auffinden noch anderweitig ermitteln ließ.

Von den 339 abgemahnten Anbietern haben zwischenzeitlich insgesamt 224 strafbewehrte Unterlassungserklärungen abgegeben. 21 Abmahnverfahren wurden eingestellt.

In zehn Fällen verweigerten Anbieter die Abgabe einer strafbewehrten Unterlassungserklärung, so dass Klage erhoben wurde. Von den zehn anhängigen Klagen sind bisher zwei im Sinne des vzbv entschieden worden.

84 eingeleitete Abmahnverfahren befinden sich noch in der Bearbeitung. Hier ist mit einem zeitnahen Abschluss zu rechnen.

Unterlassungsverfahren nach UWG und UKlaG

– Klagebefugnis

Die rechtliche Möglichkeit des vzbv, gegen solche Verstöße vorzugehen, ergibt sich aus § 13 Abs. 2 Nr. 3 UWG und §§ 3, 4 UklaG. Danach sind rechtsfähige Verbände, zu deren satzungsgemäßen Aufgaben es gehört, die Interessen der Verbraucher durch Aufklärung und Beratung wahrzunehmen und die mindestens 75 natürliche Personen oder im Bereich des Verbraucherschutzes tätige Verbände als Mitglieder haben, als sogenannte qualifizierte Einrichtungen im Sinne des § 4 des Gesetzes über Unterlassungsklagen (UKlaG) berechtigt, Unterlassungsansprüche wegen irreführender oder unlauterer Werbung sowie wegen Verstoßes gegen Verbraucherschutzgesetze geltend zu machen.

– Regelmäßige Vorgehensweise

Am Anfang eines außergerichtlichen Unterlassungsverfahrens steht eine sogenannte **Abmahnung**. Damit wird das Unternehmen aufgefordert, die beanstandete Werbung zukünftig zu unterlassen und eine strafbewehrte Unterlassungserklärung zu unterschreiben. Die Strafbewehrung durch Übernahme einer Vertragsstrafe für den Fall der Zuwiderhandlung dient dazu, die Ernsthaftigkeit des Unterlassungsversprechens zu unterstreichen und dem Abmahnenden eine Sanktionsmöglichkeit an die Hand zu geben für den Fall, dass das Unternehmen sich nicht an das Unterlassungsversprechen hält.

Im Falle der Abgabe einer Unterlassungserklärung ist das Verfahren außergerichtlich erledigt. Wird die Werbung/der Verstoß in gleicher oder im Kern übereinstimmender Form fortgesetzt, kann die in der Unterlassungserklärung übernommene Vertragsstrafe (ca. 3.000 bis 6.000 €) geltend gemacht werden. Die Zahlung erfolgt an den abmahnenden Verband.

Im Falle der Verweigerung der Unterlassungserklärung kann Klage erhoben werden. Die Klage ist darauf gerichtet, dem Unternehmen zu untersagen, künftig in der beanstandeten Form zu werben. Eingangsinstanz für die Klage ist gemäß § 24 UWG das Landgericht, in dessen Bezirk der Beklagte seine gewerbliche Nieder-

lassung hat und außerdem das Gericht, in dessen Bezirk die wettbewerbswidrige Handlung begangen worden ist. Wird also eine Werbung aus dem Ausland geschaltet, die an einen Verbraucher in Berlin gelangt, so ist in diesem Fall auch das Landgericht Berlin zuständig. Ein Unterlassungsprozess kann unter Umständen über drei Instanzen bis zum Bundesgerichtshof geführt werden. In diesem Fall beträgt die Verfahrensdauer ca. drei bis vier Jahre.

Die Prozesskosten trägt die unterlegene Partei. Ihre Höhe richtet sich nach dem Streitwert, der bei wettbewerbsrechtlichen Auseinandersetzungen durchschnittlich 15.000 € beträgt. Der vzbv verfügt über einen eigenen Prozesskostenfonds für AGB- und UWG-Unterlassungsverfahren in Höhe von derzeit 230.000 €.

Unzulässige Allgemeine Geschäftsbedingungen

Für die Überprüfung Allgemeiner Geschäftsbedingungen ist ein entsprechendes Unterlassungsverfahren in § 1 UklaG geregelt. Auch insoweit sind die Verbraucherzentralen klagebefugt. Das Verfahren dient der Bereinigung der Verträge im Vorfeld einer individuellen Auseinandersetzung.

Die Allgemeinen Geschäftsbedingungen der Anbieter im Internet waren schon mehrfach Gegenstand von Abmahnungen und Gerichtsverfahren. Allein Ende des Jahres 2002 hat der vzbv in 20 Fällen Unterlassungsverfahren nach § 1 UklaG i. V. m. §§ 307 bis 309 BGB eingeleitet. Im laufenden Jahr wurde in weiteren 15 Fällen Datenverarbeitungsklauseln im Internet wegen Verstoßes gegen die Vorschriften des TDDSG und des BDSG abgemahnt. Soweit die Verfahren nicht außergerichtlich durch Unterlassungserklärungen erledigt werden konnten, wurde in einigen Fällen Klage erhoben. In anderen Verfahren ist die Korrespondenz noch nicht abgeschlossen.

Die Klausel:

„Sollte ein bestimmter Artikel nicht lieferbar sein, senden wir Ihnen in Einzelfällen einen qualitativ und preislich gleichwertigen Artikel (Ersatzartikel) zu“

verstößt gegen §§ 475 Abs. 1, 434 BGB i. V. m. § 307Abs. 1, § 308 Nr. 4 BGB[9]. Sie gewährt dem Unternehmer das Recht, eine andere als die bestellte Ware zu liefern. Ein Leistungsänderungsvorbehalt ist in Allgemeinen Geschäftsbedingungen aber nur dann zulässig, wenn sichergestellt ist, dass die Änderungen unter Abwägung der beiderseitigen Interessen für den Verbraucher zumutbar sind. Auch wenn der gelieferte Artikel preislich und qualitativ gleichwertig ist, muss das Abweichen von der versprochenen Leistung nicht per se zumutbar sein. Die Lieferung eines gänzlich anderen Produkts stellt eine erhebliche Abweichung von der versprochenen Leistung dar.

9 LG Hamburg, Urteil vom 5. 9. 2003–Az. 324 O 224/03 –, nicht rechtskräftig.

Die Klausel :

„Alle vom Kunden erhaltenen Daten werden ausschließlich erhoben, verarbeitet, genutzt und an beauftragte Partner weitergeleitet, soweit dies für die Begründung und Durchführung … der weiteren Geschäftsbeziehung zwischen dem Kunden und der…erforderlich ist“

verstößt gegen § 307 Abs. 1, 2 Nr. 1 BGB i. V. m. §§ 3, 5, 6 TDDSG. Sie gibt keinen Aufschluss darüber, ob es sich bei den „weiteren Geschäftsbeziehungen“ um bereits bestehende oder von der Verwenderin erhoffte zukünftige Beziehungen handeln soll (Marketingzwecke). Es wurde eine Unterlassungserklärung abgegeben.

Erfahrungen beim Online-Einkauf

Folgende Mail eines Verbrauchers erreichte uns in den letzten Tagen. Sie schildert ein typisches Problem:

Hallo,
ich habe folgendes Problem mit einer Internetfirma namens . . . .:
Ich habe am 14. 10. 03 also morgen vor 6 Wochen ein PC-System im Wert von 560 Euro bestellt und per Vorkasse bezahlt. Leider habe ich bis heute keine Lieferung von der Firma erhalten. Auf Email wird nicht geantwortet und telefonisch ist niemand erreichbar.
Ich habe jetzt natürlich den Verdacht, dass es sich um eine Briefkastenfirma handelt. Mittlerweile habe ich von mehreren Kunden der Firma erfahren, dass sie das gleiche Problem haben.
Meine Frage: Ist Ihnen vielleicht die Firma bekannt?
Wie soll ich mich jetzt verhalten?

Vielen Dank für Ihre Hilfe.
Mit freundlichen Grüßen

EU-weites Einkaufen im Netz ist mit weiteren Hindernissen verbunden. Das belegt eine im Mai 2003 veröffentlichte Studie des bei der Verbraucherzentrale Nordrhein-Westfalen angesiedelten Europäischen Verbraucherzentrums (EVZ) in Düsseldorf[10]: Oft stürzten die Tester bei ihren 114 grenzüberschreitenden Ein-

10 In Deutschland gibt es ein EVZ in Düsseldorf und ein EVZ in Kiel. „Das Netz der Europäischen Verbraucherzentren (EVZ-Netz) ist ein wichtiges Bindeglied zwischen der Kommission und den europäischen Verbrauchern. Die Rolle des Netzes besteht darin, die europäischen Verbraucher dabei zu unterstützen, ein besseres Verständnis dafür zu bekommen, wie sie sich den Binnenmarkt zu Nutze machen können sowie sie bei Problemen zu beraten. Dadurch soll erreicht werden, dass sie sich beim Einkauf in einem anderen Land genauso sicher fühlen wie in ihrem eigenen Land. Eine weitere wichtige Aufgabe des Netzes ist es, die EU-Kommission mit wesentlichen Basisinformationen über die Belange der Verbraucher zu versorgen.“ Der Text und weitere Informationen sind nachzulesen bei der EU-Kommission: http:/www.europa.eu.int/comm/consumers/redress/compl/euroguichet/index_de.htm

kaufsversuchen schon bei der Bestellung ab.[11] In 21 Fällen wurde zwar der Auftrag bestätigt, auf die Lieferung warteten sie jedoch vergeblich. In neun Fällen folgte zwar die Rechnung, aber keine Ware. Nur 57 % der Bestellungen liefen glatt.

Das nächste Problem entstand bei der Lieferung: Nur zwei Drittel der Produkte von T-Shirts bis zu Druckerpatronen wurden tatsächlich geliefert. Die durchschnittliche Lieferungsdauer betrug elf Tage.

Bei der Rückgabe von 57 der 75 gelieferten Produkte taten sich neue Hindernisse auf: Obwohl Kunden nur zur Erstattung der gewöhnlichen Kosten für die Rücksendung (bei einem Bestellwert bis zu 40 €) verpflichtet werden dürfen, erstatteten nur 21 Anbieter die übrigen Kosten, in 18 Fällen gab es gar kein Geld zurück. Außerdem fiel den Testern auf, dass die meisten Online-Angebote nur auf Kunden im eigenen Land abzielen. So informierte von den 262 getesteten Seiten nur rund ein Viertel in einer anderen als der Landessprache.[12]

CI- Studie: Credibility on the web[13]

Als Quelle für unabhängige Verbraucherinformation ist das Internet mit Vorsicht zu genießen. Das ist das Ergebnis einer Studie, die Consumers International, die Dachorganisation von 250 Verbraucherorganisationen in 115 Ländern, Anfang November 2002 veröffentlicht hat. Die Untersuchung, an der Verbraucherorganisationen aus 13 Ländern, darunter der vzbv, beteiligt waren, bezog sich auf insgesamt 460 Websites, davon 33 aus Deutschland. Untersucht wurden Verbraucherinformationen zu Gesundheit und Finanzdienstleistungen im Internet, die sich leider häufig als lückenhaft und unpräzise erwiesen haben. Ziel der Untersuchung, die auch von der Europäischen Kommission unterstützt wurde, war es, Verbrauchern Kriterien an die Hand zu geben, um damit zwischen glaubwürdiger Information und kommerziell beeinflussten Inhalten unterscheiden zu können. Untersucht wurden Informationsseiten, die im Vorfeld einer Kaufentscheidung Informationen für Verbraucher bereithalten. Im Bereich Gesundheit waren die Websites mit Informationen über Brust- und Prostatakrebs sowie über Allergien. Im Bereich der Finanzdienstleistungen wurden Informationen zu Hypothekendarlehen und Lebensversicherungen geprüft. Zusätzlich wurden Preisvergleiche über Computer, Flüge oder Mietautos untersucht. Dabei wurden u. a. folgende gravierende Mängel festgestellt:

– Bei 60 % der Sites fehlten Informationen, ob ihr Inhalt von kommerziellen Interessen beeinflusst ist oder nicht;
– nur 41 % der Sites, die Produkte empfahlen, machten Angaben über die Quellen der Preise;

11 vwd/28. 5. 2003/AFP/fh.
12 Die gesamte Studie ist abrufbar unter www.europaeisches verbraucherzentrum.de
13 www.consumersinternational.org

– 55 % der Sites sagten nichts über die Aktualität ihres Inhalts aus;
– mindestens 50 % der Websites, die in medizinischen oder finanziellen Fragen Rat boten, gaben keine vollständige Information über Autorität und Qualifikation der dahinter stehenden Personen;
– auf 30 % der Sites waren weder eine Kontaktadresse noch eine Telefonnummer zu finden.

Sicherheit von Zahlungen

Die Verbraucher müssen überzeugt sein, dass elektronische Zahlungen keine „Mühe“ machen, wird der für den Binnenmarkt zuständige EU-Kommissar Bolkestein bei der Veröffentlichung einer EU-Studie im September dieses Jahres zitiert.[14] Im Jahr 2001 seien in der EU an jedem Werktag über 207 Millionen bargeldlose Zahlungen durchgeführt worden, was pro Einwohner und Jahr 139 sind. Ein erheblicher Anteil dieser Zahlungen ist dabei nach Darstellung der EU elektronisch erfolgt.

Generell vertrauen der Studie zufolge Konsumenten in den skandinavischen Ländern dem E-Commerce eher als Verbraucher im Süden. Was die Sicherheitsinformationen auf untersuchten 600 Websites betrifft, stellte die EU-Studie ebenfalls erhebliche Unterschiede und teils gravierende Mängel fest: So waren nur auf etwas mehr als einem Viertel der 600 untersuchten E-Commerce-Websites Sicherheitsinformationen ohne weiteres auf der Website selbst zu finden. Die französischen Websites schnitten mit 47 Prozent noch am besten ab, österreichische Websites lieferten dagegen mit sechs Prozent den schlechtesten Wert. Große Unterschiede gibt es auch hinsichtlich der Verständlichkeit der Sicherheitsinformationen zwischen E-Commerce und E-Banking. Demnach bieten EU-weit 83 Prozent der geprüften E-Banking-Sites klar verständliche Informationen, während dies bei den E-Commerce-Websites nur bei 55 Prozent der Fall ist.

Praktische Sicherheitsvorkehrungen bei Internet-Auktionen bestehen in der Einrichtung von Treuhandkonten. Die Firma eBay bietet einen solchen Service gegen Aufpreis an. Damit sichergestellt ist, dass Kunden, die bereits im Voraus gezahlt haben, nicht leer ausgehen, wird das Geld erst freigegeben, wenn der Kunde die Ware tatsächlich erhalten hat. Die Akzeptanz dieses vom Ansatz her sehr zu begrüßenden zwischengeschalteten Verfahrens wird zum einen von der Zuverlässigkeit des Treuhänders, aber auch davon abhängen, dass keine oder nur geringe zusätzliche Kosten für die Verbraucher entstehen.

Spamming

Ein besonderes Ärgernis nicht nur aus der Sicht der Verbraucher stellen unverlangte Werbemails dar. Der Transatlantische Verbraucherdialog TACD (Trans-

14 http:/www.e-business.de/texte/8981.asp

atlantic Consumer Dialogue)[15], ein Forum für 65 europäische und amerikanische Verbraucherorganisationen, führt zur Zeit eine Online-Befragung von Verbrauchern nach ihren Erfahrungen durch, deren Ergebnis im Februar 2004 der OECD sowie der internationalen Presse vorgestellt werden soll.[16]

Die Datenschutzrichtlinie für elektronische Kommunikation vom 12. Juli 2002[17] schreibt vor, dass elektronische Post für die Zwecke der Direktwerbung nur bei vorheriger Einwilligung der Teilnehmer gestattet werden darf. Die Richtlinie wird voraussichtlich im Frühjahr 2004 durch die Novelle des Gesetzes gegen den unlauteren Wettbewerb (UWG) umgesetzt werden.

Es wird abzuwarten sein, ob das jüngst vom amerikanischen Abgeordnetenhaus verabschiedete Gesetz, das Geldstrafen für Spam-Versender vorsieht, die gewünschte abschreckende Wirkung erzielen wird.

Zwischenbilanz und Ausblick

Die Europäische Kommission hat am 21. November 2003 einen ersten Bericht über die Anwendung der E-Commerce-Richtlinie veröffentlicht[18]. Darin kommt sie zu dem vorläufigen Ergebnis, dass aufgrund der ihr vorliegenden Informationen derzeit kein Bedarf für eine Anpassung der Richtlinie besteht. Da die Richtlinie noch nicht in allen Mitgliedstaaten umgesetzt ist, wäre eine Überarbeitung derzeit auch noch verfrüht. Der elektronische Geschäftsverkehr sei jedoch ein sich schnell entwickelnder Bereich, der ständig beobachtet und analysiert werden müsse. Die Konsultation ist also weiterhin offen. Im Jahr 2005 soll ein zweiter Erfahrungsbericht vorgelegt werden.

In der Zwischenzeit will die Kommission sich dafür einsetzen, z. B. durch Maßnahmen zur technischen Unterstützung die Sicherheit von Zahlungen zu verbessern.

Darüber hinaus soll die Online-Streitbeilegung gefördert werden. Den schon erwähnten Europäischen Verbraucherzentren sowie den Clearingstellen[19] kommt in Bezug auf die grenzüberschreitenden Streitigkeiten eine besondere Bedeutung

15 Der Transatlantische Verbraucherdialog (TACD) wurde 1998 gegründet. Das Forum erarbeitet und beschließt gemeinsame verbraucherpolitische Empfehlungen für die amerikanische Regierung und die EU-Kommission, um die Interessen der Verbraucher in der Politik der EU und der USA und in globalen Fragen geltend zu machen. TACD erhält von der Kommission finanzielle und organisatorische Unterstützung. Näheres unter www.europa.eu.int;www.tacd.org

16 http:/www.net-consumers.org/erica/spamsurvey.htm.

17 Amtsblatt EG Nr. L 201/37 v. 31. 7. 2002.

18 http:/www.europa.eu.int/comm/internal_market/en/ecommerce/com2003–702/com2003–702_de.pdf

19 Das Netz umfasst alle 15 Mitgliedstaaten sowie Norwegen und Island. Das Netz befasst sich mit jeder Art von Rechtsstreitigkeit zwischen einem Verbraucher und einem Gewerbetreibenden über Waren und Dienstleistungen, ebenso wie Lieferungen, beschädigten Waren oder Waren oder Dienstleistungen, die nicht der Beschreibung entsprechen. Das EEJ-NET wird durch das FIN-

zu. Die deutsche Clearingstelle ist bei der deutsch/französischen Beratungsstelle in Kehl angesiedelt.[20]

Schließlich erwägt die Kommission zur Stärkung des Vertrauens in den Online-Handel die Annahme einer Empfehlung auf der Grundlage der vom Europäischen Verbraucherverband BEUC und der Union der Industrie- und Arbeitgeberverbände UNICE gemeinsam geleisteten Arbeit zur Entwicklung von Standards für vorbildliche Gütesiegel. Gibt es nämlich zu viele Verhaltenskodizes, Trustmarks (Vertrauensmarken) und sonstige Gütezeichen, können Verbraucher eher verwirrt werden als hierdurch eine Orientierung zu erfahren.[21]

Die Verbraucherverbände sind in die politische Diskussion eingebunden, auf europäischer Ebene über den Verbraucherverband BEUC, international durch Beteiligung an dem transatlantischen Verbraucherdialog. Wir werden uns weiterhin für die Stärkung der Rechte der Verbraucher bei der Nutzung des Internet und anderer moderner Medien einsetzen, um auf diese Weise dazu beizutragen, das Vertrauen in den elektronischen Handel dauerhaft und effektiv zu stärken.

NET ergänzt, das sich ausschließlich mit Verbraucherrechtsstreitigkeiten im Bereich der Finanzdienstleistungen (Kredit, Geldanlage, Darlehen usw.) befasst. Näheres unter: www.eejnet.org

20 www.euroinfo-kehl.com

21 Einen Überblick über empfehlenswerte Gütesiegel in Deutschland gibt es unter www.initiativ-ed21.de

Sicheres Handeln bei eBay

Jörg Rheinboldt

Sehr geehrte Damen und Herren. Sicher handeln bei eBay; ich werde sehr wenig über IT-Technologie sprechen, sondern darüber: Was macht eBay, um Sicherheit und Vertrauen auf dem Marktplatz zu garantieren? Wie handelt man als eBay-Nutzer sicher? Zunächst werde ich Ihnen kurz den Marktplatz eBay vorstellen, auf dem wir den Ansatz „Transparenz schafft Vertrauen“ umsetzen, denn Vertrauen und Sicherheit sind fundamental wichtig für einen Marktplatz wie eBay.

Unsere Mitglieder können sich bei uns selber aussuchen, welchen persönlichen Sicherheits- und Vertrauenslevel sie bei ihren Transaktionen wählen wollen. Weiterhin zeige ich die Sicherheitsmechanismen auf, die wir auf der Plattform einsetzen, um den Handel sicher zu machen. Mit einem kurzen Fazit möchte ich schließen.

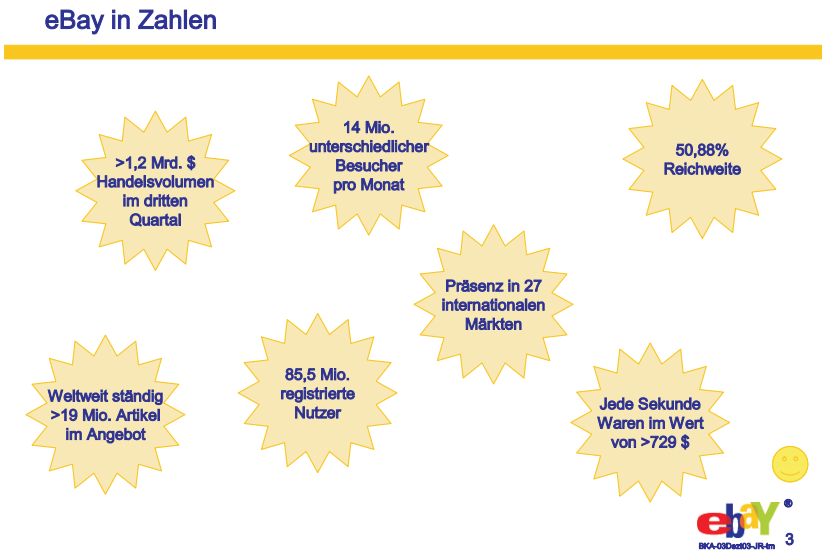
Unsere Mission ist die Bereitstellung eines Marktplatzes, auf dem fast jeder fast alles handeln kann. Ich bin bei eBay für das Thema Sicherheit und Vertrauen zuständig und kümmere mich darum, wer bei uns eigentlich nicht handeln soll und was man bei uns nicht handeln darf.

Wir sind inzwischen in 27 Ländern weltweit präsent; Afrika und Russland sind noch ein weißer Fleck auf unserer Landkarte.

Ist bei der eBay GmbH für die Sicherheit zuständig: Jörg Rheinboldt

Unser Ansatz heißt: Wir bauen einen Marktplatz, der offen ist für alle. Jeder, der einen Internetanschluss hat, kann bei uns handeln. Das sind im Moment 75 Mio. registrierte Nutzer weltweit.

Die folgenden Zahlen geben einen Überblick über die Dimension des Marktplatzes.



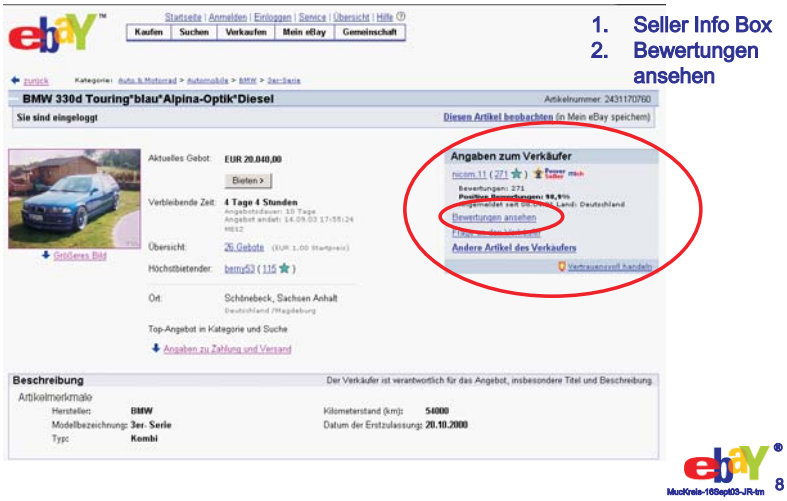
Grundlegendes Prinzip unseres Marktplatzes ist es, das er ein Level-Playing-Field ist. Das bedeutet: alle Verkäufer und Käufer haben die gleichen Rechte, alle haben die gleichen Pflichten und alle haben die gleichen Preise. Wenn z. B. der private Jörg Rheinboldt seinen Laptop bei eBay verkauft, zahlt er genauso viel Einstellgebühren wie ein großer Computerhersteller, der auf die Idee kommt, eBay als weltweiten Vertriebskanal zu nutzen. Es ist eines der offenen Geheimnisse unseres Erfolgs, dass wir nie davon abrücken, dass für alle die gleichen Regeln gelten. Ein weiterer Eckpfeiler unseres Marktplatzes ist die nachhaltige Förderung der Handelskompetenz unserer Mitglieder: Vertrauen und Sicherheit auf unserem Marktplatz manifestiert sich auch darin, dass die Menschen, die bei uns handeln, vernünftig mit ihrer Verantwortung umgehen können. Als Marktplatzbetreiber sehen wir unsere Aufgabe darin, mittels präventiver und repressiver Maßnahmen sicherzustellen, dass die Rahmenbedingungen für den Handel stimmen und diese kontinuierlich verbessert werden.

Transparenz schafft Vertrauen. Unsere Aufgabe ist, Transparenz zu schaffen, dass die Nutzer qualifizierte Entscheidungen treffen können.

Transparenz erreichen wir, indem wir die Fülle an Informationen auf dem Marktplatz über Artikel, Preise und Nutzer strukturieren. Das bedeutet zum einen, dass alle Artikel in Kategorien eingeteilt sind. Die Kategorienstruktur ist beliebig erweiterbar. Inzwischen sind es über 10.000, weil auf dem Marktplatz immer mehr Produkte gehandelt werden.

Weiterhin gibt eine Basissuche und eine erweiterte Suche, in der man nach beliebigen Stichwörtern suchen kann. Die Basisinformationen und -funktionalitäten für Käufer und Verkäufer liefern die Grundlagen für den richtigen und sicheren Handel bei eBay. In den aktuellen Angeboten weisen wir auf Artikel hin, die im Moment entweder besonders viel oder günstig gehandelt werden Die Art und Weise der Präsentation optimieren wir permanent, um den Anforderungen unserer Nutzer gerecht zu werden. Die Marktforschung ist hier ein zentrales Instrument.

Informationen über Artikel

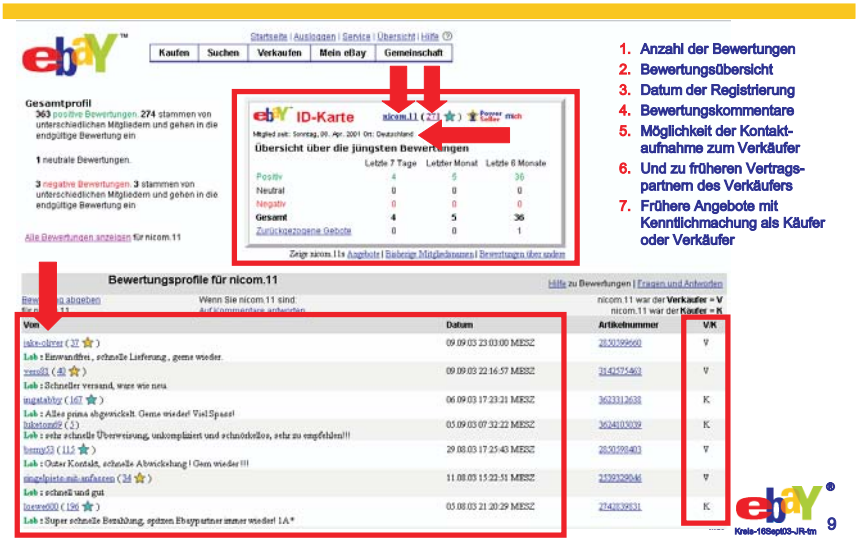


Ich möchte Ihnen nun am Beispiel eines Autokaufs demonstrieren, wie der Ablauf einer Transaktion aussieht und welche Services bei eBay verfügbar sind, damit sich jedes Mitglied den seinen individuellen Sicherheitsbedürfnissen entsprechenden Level wählen kann.

Wir haben einen 3er BMW ausgesucht und wollen uns erst einmal darüber informieren, was das für ein Auto ist. Wir sehen, dass er im Moment 20.040 € kostet. Die Auktion läuft noch vier Tage und vier Stunden. Mehrere Leute haben schon darauf geboten. Der BMW hat 54.000 km und ist in 2000 zugelassen worden. Innerhalb kürzester Zeit kennen wir die Basisdaten des Artikels.

Weiterhin wichtig ist nun zu wissen, wer den BMW eigentlich verkauft, denn nicht eBay ist der Verkäufer, sondern ein meist unbekannter Dritter. Über diesen Verkäufer finden wir Informationen in der so genannten Seller Infobox. Diese Seller Infobox finden wir rechts, wo der rote Kreis erschien. Bei den Angaben zum Verkäufer sehen wir, welches Pseudonym hinter dem Verkäufer steht und wie viele Transaktionen diese Person bei eBay bereits getätigt hat: in unserem Fall sind das über 200. Dann kann man noch viel genauer anschauen, welche Verkäufe und mit welchen Käufern dieser Verkäufer bereits absolviert hat, indem ich auf „Bewertungen ansehen“ klicke.

Informationen über Verkäufer und Käufer



Das Bewertungsforum sind die Informationen über alle Transaktionen, die das Mitglied in der Vergangenheit getätigt hat, bewertet von allen Transaktionspartnern. Man sieht in einer übersichtlichen ID-Karte, wie viele Bewertungen der Verkäufer hat, wie viele Transaktionen in den letzten sieben Tagen, im letzten Monat, in den letzten sechs Monaten vorgenommen wurden, wann und in welchem Land der Verkäufer sich registriert hat und bei weiterem Interesse die Kommentare der einzelnen Transaktionspartner, also ob sie mit dem Verkäufer zufrieden waren, positiv, neutral, negativ und in welchem Verhältnis die zueinander standen. Für weitergehende Fragen kann ich als Käufer direkt per e-mail Kontakt zum Verkäufer und zu früheren Vertragspartnern des Verkäufers aufnehmen. Wenn ich das auf die Offline-Welt übertrage, ist das etwas Besonderes. Nehmen sie ein Einzelhandelsgeschäft: hier ist es für den Käufer sehr schwierig, sich Informationen darüber zu besorgen oder zu beschaffen, wer in der Vergangenheit alles gekauft hat und wie zufrieden die Leute mit ihren Käufen waren. Bei eBay ist das extrem transparent – sowohl für unseren unbekannten „nicom11“ als auch für bekannte Verkäufer wie z. B. Quelle.

Wir versuchen, es unseren Mitgliedern, die bei uns handeln, möglich zu machen, dass sie sich ihren eigenen Sicherheits- und Vertrauenslevel einstellen können. Das tun wir dadurch – jetzt am Beispiel Auto –, dass wir verschiedene Services bieten, mit denen man sich absichern kann und ohne böse Überraschungen seinen BMW nach erfolgter Bezahlung auch erhält. Bei eBay ist es in der Regel so, dass sich Verkäufer und Käufer in den seltensten Fällen gegenüberstehen und der Käufer das Auto nicht persönlich in Augenschein nehmen kann. Es ist daher wahr-

scheinlich, dass der Käufer nicht einfach auf „Kaufen“ klickt, das Geld im Briefumschlag verschickt und sich das Auto schicken lässt. Es ist davon auszugehen, dass er noch mehr über das Auto wissen möchte. Er kann z. B. prüfen lassen, ob die Beschreibungen in der Artikelbeschreibung wirklich auf das Auto zutreffen, d. h. er könnte einen eBay Car-Check, den wir in Zusammenarbeit mit A. T. U. Auto-Teile-Unger anbieten und der das Produkt authentifiziert, verlangen.

Tool Box für die Individuelle Gestaltung von Sicherheitsstufen beim Autokauf

Produkt-Authentifizierung

MucKrete-18Sept03-JR-tm 11

Tool Box für die Individuelle Gestaltung von Sicherheitsstufen beim Autokauf

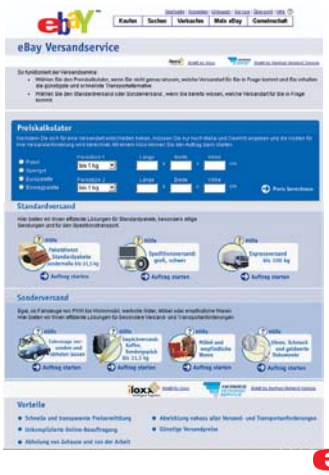
Gebrauchtwagenpreischeck

MucKrete-18Sept03-JR-tm 12

Weiterhin kann er einen Gebrauchtwagenpreischeck durchführen …

Tool Box für die Individuelle Gestaltung von Sicherheitsstufen beim Autokauf

Lieferservice



13

… oder einen Lieferservice beauftragen.

Das sind alles Services, die wir anbieten, wenn es alleine um den Verkauf von Autos geht.

Tool Box für die Individuelle Gestaltung von Sicherheitsstufen beim Autokauf

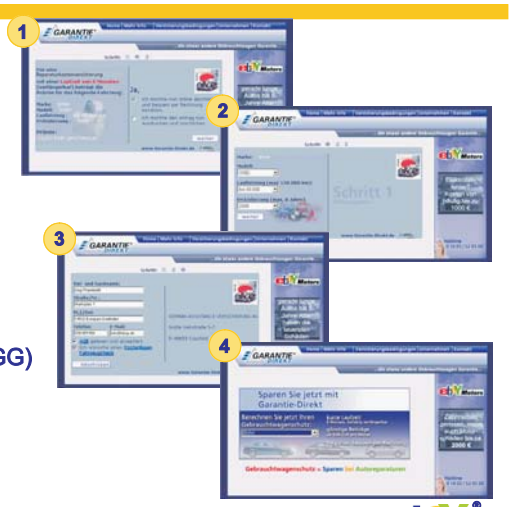
Treuhandservice

14

Natürlich kann – wie bei allen anderen Transaktionen auch – ein Treuhandservice eingeschaltet …

Tool Box für die Individuelle Gestaltung von Sicherheitsstufen beim Autokauf

Garantie/Umtausch (GGG)



MuckRels-16Sept03-JR-tm 15

… oder eine Garantie bzw. eine Rückgabegarantie vereinbart werden.

Tool Box für die Individuelle Gestaltung von Sicherheitsstufen beim Autokauf

"Geprüftes Mitglied"

MuckRels-16Sept03-JR-tm 16

Über den Service „geprüftes Mitglied“, bei dem sich jedes Mitglied über den PostIdent-Prozess authentifizieren lassen kann, erhöht sich die Vertrauenswürdigkeit des einzelnen Mitglieds.

Tool Box für die Individuelle Gestaltung von Sicherheitsstufen beim Autokauf

“Käuferschutzprogramm”

„Last but not least“: das Käuferschutzprogramm deckt den Fall ab, wo eine Transaktion fehlgeschlagen ist, d. h. z. B. der Verkäufer, trotz Bezahlung, nicht geliefert hat. Dieses Programm greift nur bis zu einem Betrag von 200 €.

Die Sicherheitsmechanismen auf der Plattform laufen je nach Stadium der Transaktion zum größten Teil automatisch ab.

Marktplatz-Sicherheit - Prävention

Prävention

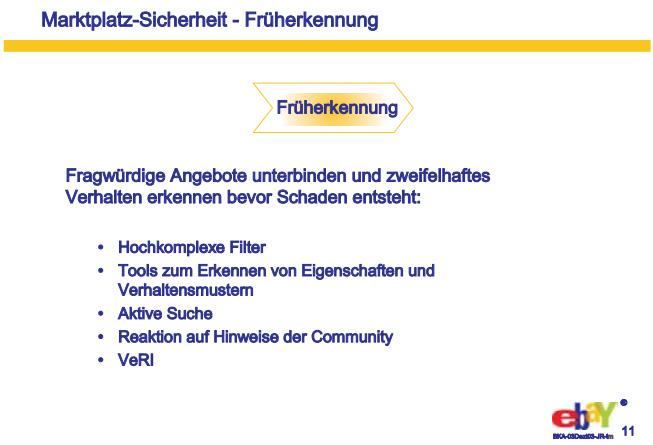
Durch Aufklärung und verantwortungsvolles Verhalten verhindern dass Schaden entsteht

- Aufklärung
- Bewertungsforum
- Verifizierung der Anmeldeinformationen
- "Geprüftes Mitglied"
- Services (z.B. Treuhand- und Lieferservices)
- Zusammenarbeit mit Strafverfolgungsbehörden, Behörden und Non-Governmental Organisations (Filter/Suchbegriffe)

Im Bereich der Prävention liegen meines Erachtens die effektivsten Tools, da sie dazu beitragen, dass gar nicht erst etwas auf die Plattform kommt, was dort nicht hingehört. In Zusammenarbeit mit der Schufa führen wir eine Verifizierung der Anmeldeinformation durch, bei der Vorname, Name und Adressinformationen überprüft werden. Den Service „geprüftes Mitglied" haben sie ja bereits bei unserem virtuellen Autokauf kennen gelernt. Wir betreiben eine Menge Aufklärung. Das ist nur ein Wort, aber ein sehr interessanter Bereich, wo wir dynamisch Informationen einblenden für Nutzer in bestimmten Situationen. Wenn Sie z. B. auf eine Kamera bieten, die in Japan ist und Sie in Deutschland sind, dann würden wir Sie darauf hinweisen, dass Sie gerade auf eine Kamera bieten, die in Japan ist und Sie fragen, ob Sie sich Gedanken darüber gemacht haben, dass vielleicht der Postversand etwas kompliziert werden könnte. Bei einem Klavier würden wir Ihnen das wahrscheinlich sogar mehrfach einblenden.

Neben diesen praktischen Hinweisen, die auf Aspekte aufmerksam machen, die möglicherweise Ursache für den Fehlschlag einer Transaktion sein können, werden auch Warnmitteilungen eingeblendet, wenn Verkäufer einen Artikel listen wollen, der möglicherweise problematisch sein könnte. Sie räumen z. B. Ihren Dachboden auf und finden den ausgestopften Dachs ihrer Vorfahren, den sie aus Platzmangel sofort bei eBay zum Verkauf einstellen. Hier weisen wir sie darauf hin, dass dieses Tier möglicherweise gerade in dem Bundesland, wo Sie wohnen, gar nicht gehandelt werden darf.

Das Aufspüren solch fragwürdiger Artikel übernimmt bei eBay eine Kombination aus Maschine und Mensch. Bei der großen Anzahl der gelisteten Artikel sind wir natürlich auf Expertensachverstand und -wissen angewiesen. Daher arbeiten wir eng zusammen mit Strafverfolgungsbehörden, mit Bundes- und Landesbehörden sowie Interessengruppen daran, unsere Mitarbeiter zu trainieren, unsere Warnmechanismen zu verbessern und vor allen Dingen unsere Mitglieder darüber aufzuklären, wie man sicher handeln kann.



Zum Zeitpunkt zwischen Angebotseinstellung und möglichem Abschluss einer Transaktion sorgen wir im Rahmen der Früherkennung dafür, dass wir erkennen falls etwas oder jemand auf der Plattform ist, das oder der nicht da sein soll. Hier haben wir in den letzten 20 Monaten über 10 Mill. US-Dollar investiert und haben in Deutschland über 100 Mitarbeiter, die sich um Vertrauen und Sicherheit auf der Plattform kümmern.

Zum Zeitpunkt nach Abschluss der Transaktion unterstützen wir im Falle eines Missbrauchs die Strafverfolgungs- und Aufsichtsbehörden, um Fälle aufzuklären.

Das Fazit ist: Vertrauen und Sicherheit im Internet zu erreichen, kann nur dann glücken, wenn alle Beteiligten die ihnen zustehende Verantwortung nachhaltig übernehmen und von den Möglichkeiten, die das Internet bzw. ein Marktplatz wie eBay bietet, auch Gebrauch machen. Für eBay ist die Zusammenarbeit mit Strafverfolgungsbehörden daher ein Thema von herausragender Bedeutung.

Vielen Dank.

Zukunftsperspektiven: Wirtschaftliche Entwicklung und IT-Sicherheit

David Finn

Vielen Dank für die einführenden Worte! Es ist für mich eine Ehre, heute hier zu sein, insbesondere, da heute mein Geburtstag ist.

Ich möchte mit einer kleinen Geschichte einsteigen. Vor etwa sechs, sieben Jahren war ich Staatsanwalt und hatte gerade ein Verfahren abgeschlossen, wollte mich für drei Wochen in den Urlaub begeben und hatte mich mit einem Wirtschaftskriminellen zu befassen, der fünf bis sechs Millionen Dollar auf seine Seite gebracht hatte. Ich saß im Taxi auf dem Weg zum Flughafen. Der Taxifahrer hat mich in ein Gespräch verwickelt und mich gefragt, was ich beruflich mache. Ich erklärte es ihm. Ich sagte ihm, dass ich gerade eine sehr schwierige Ermittlungsarbeit abgeschlossen hatte und dass es sich um ein Betrugsverfahren im Bereich Wirtschaftskriminalität handelte und dass ich sehr glücklich war, weil ich es geschafft hatte, den Täter dingfest zu machen.

Der Taxifahrer fragte mich, ob wir etwas von dem Geld gefunden hätten. Ich sagte: „Nein, wir haben uns um das Geld nicht so sehr gekümmert. Meine Aufgabe war es, die Personen zu ermitteln und vor Gericht zu bringen. Es war einfach nicht der Schwerpunkt meines Interesses während der Ermittlungen." Der Taxifahrer fragte, wie hoch das Strafmaß sein würde. Ich erklärte ihm, dass das Strafmaß erst in einigen Wochen festgesetzt werden würde. Aber ich sagte ihm, dass ich schätzte, dass er etwa fünf Jahre Freiheitsstrafe bekommen würde. Der Taxifahrer hielt einen Moment inne und sagte: „Für fünf, sechs Jahre würde ich auf jeden Fall ins Gefängnis gehen, wenn ich dafür auch fünf bis sechs Millionen Dollar bekäme." Ich habe viele Menschen kennen gelernt und von vielen Menschen viel gelernt. Auch von diesem Taxifahrer habe ich etwas gelernt. Ich hatte dann eine sehr gute Urlaubszeit. Ich habe darüber nachgedacht, was der Taxifahrer und ich besprochen hatten. Später musste ich noch oft an dieses Gespräch denken. Immer, wenn ich einen Betrugsfall hatte, habe ich mir viel mehr Gedanken darüber gemacht, wie ich an das Geld des Straftäters herankommen würde. Das ist auf diese kleine Geschichte mit dem Taxifahrer zurückzuführen.

Einige Jahre später wurde ich von Microsoft eingestellt. Natürlich war man dort an meinem Hintergrundwissen im Bereich Kriminalitätsbekämpfung interessiert. Das heißt natürlich nicht deshalb, weil ich selbst ein Straftäter gewesen wäre, sondern weil ich wusste, wie man Straftäter dingfest macht. Ich werde noch über Kriminelle und über hochkarätige Betrugsstraftäter sprechen. Ich habe mir dann Gedanken darüber gemacht, wie wir es schaffen können, diese Wirtschaftskriminellen dingfest zu machen und auch an deren Geld, an deren Vermögen heran zu kommen. Das ist ein sehr wichtiger Punkt aus meiner Sicht. Meine Aufgabe bei Microsoft ist es sicherlich auch, Personal einzustellen. Das Personal, das

für uns interessant ist, ist auch das Personal, das hier heute versammelt ist. Das heißt, wir haben viele ehemalige Polizeibeamte, ehemalige Staatsanwälte, die sehr hart gearbeitet haben, um Straftäter festzunehmen und vor Gericht zu bringen.

David Finn von Microsoft berichtete über Zukunftsperspektiven im IT-Bereich

Während meiner Tätigkeit bei Microsoft habe ich früh gelernt, dass Straftäter sehr häufig weder ins Gefängnis kamen noch ihr Geld verloren haben. Ich habe 1999 bei Microsoft angefangen. Es gab in dieser Zeit einen schweren Raubüberfall in Schottland. Der Inhaber einer Firma wurde mit Waffengewalt gezwungen, CD-ROMs und auch Eigentumszertifikate für diese Software herauszugeben. Die Täter haben den Inhaber gefesselt und geknebelt und jede Menge Zertifikate und Software dieser Firma geraubt. Sehr oft haben wir bei unserer Arbeit keinen Erfolg und sehr häufig sind die Täter nach einem solchen Vorfall immer noch flüchtig. Ich habe dann von einem weiteren Fall erfahren, bei dem im Vereinigten Königreich sehr viele Polizeidienststellen mit gestohlener Software ausgestattet wurden. Die Polizei hat dann hervorragende Arbeit geleistet. Es wurden sehr viele Täter festgenommen. Der Fall wurde vom Gericht abgewiesen und das Verfahren eingestellt.

Das war aus verschiedenen Gründen sehr unerfreulich für Microsoft. Die gefälschte Software, die benutzt worden war, stützte sich auch auf die Software und auf die Zertifikate, die in dem Fall in Schottland gestohlen worden waren. Das heißt, dass die Strafverfolgungsbehörden, die eigentlich Straftäter verfolgen

müssen, selbst mit gestohlener Software und mit gestohlenen Zertifikaten ausgestattet waren und damit arbeiteten. Das war eine sehr unerfreuliche Sache. Die Personen, die falsche Software herstellen, sind oftmals andere als die, die die Zertifikate herstellen. Es gab dann noch ein weiteres Verfahren, das sich mit diesem zweiten Aspekt dieses Verfahren befasste – das heißt, dem Herstellen falscher Zertifikate.

Hier noch ein weiterer Fall, bei dem eine Computerfirma in Irland ausgeraubt wurde. Dabei wird ein Bezug hergestellt zur Irish Republican Army. Es ist zu vermuten, dass die IRA bei diesem Raubüberfall eine Rolle spielte. Auch hier ging es um den Raub von Software. Und auch hier gab es keinerlei Verurteilungen. Das heißt, als ich bei Microsoft angefangen habe, hatten wir die Situation, dass in solchen Fällen sehr häufig keine Strafen verhängt wurden.

Ich möchte noch einmal verdeutlichen, warum sich so viele Straftäter im Bereich Computerpiraterie betätigen. Ein Beispiel: Man schätzt, dass der Straßenwert für 1 kg Kokain bei 30.000 Pfund liegt. Man kann dieses Kokain auf der Straße für etwa 60.000 Pfund verkaufen. Die Gewinnspanne ist also 100 %. Wenn man sich im Vergleich dazu den Softwarebereich anschaut, dann kann man davon ausgehen, dass der Straßenwert bei 300.000 Pfund liegt im Vergleich zu 30.000 Pfund im Einkauf. Das heißt, hier ist die Gewinnspanne um das Zehnfache höher. Folglich gibt es im Bereich der Herstellung falscher Software größere Gewinnspannen als im Drogenbereich. Die Hersteller und die Verteiler falscher Software sind sehr schwer zu finden. Man hat häufig in der mittleren Organisationsebene Straftäter, die sehr clever sind und es immer wieder schaffen, den Strafverfolgungsbehörden zu entkommen.

Ein anderer interessanter Punkt beim Vergleich zwischen Softwarepiraterie und Drogen ist ebenfalls ein finanzieller Aspekt. Normalerweise hat man es mit relativ simplen Fälschungen zu tun. So sind Fälschungen auf der Straße sehr günstig zu bekommen. Ich bin mehr interessiert an den wirklich großen Fälschungsdelikten. Man braucht 1 bis 2 Millionen Pfund, um eine Fabrik auf die Beine zu stellen, in der Software professionell gefälscht werden kann. Außerdem braucht man ein sehr großes Maß an Know-how. Es kostet viele Ressourcen, eine Fälscherwerkstatt, eine Fälscherfabrik, auf die Beine zu stellen. Wir haben festgestellt, dass sich immer mehr Firmen Richtung Osten verlagert haben. Man sieht einiges in Westeuropa, auch einiges in den Vereinigten Staaten. Aber so wie es früher war, dass man einen Container voller falscher Software hatte, den man dann sicherstellen konnte, das ist heute nicht mehr so. Die Täter sind schlauer geworden. Und sie wählen andere Verpackungsgrößen, um die gefälschte Software zu verteilen. Es gibt eine Reihe von mobilen Einrichtungen, wie zum Beispiel Wohnwagen, die schnell von einem Ort an einen anderen verlegt werden können und von den Tätern genutzt werden, um die Strafverfolgung zu erschweren.

Es gibt sehr viele organisierte Kriminelle, die sich mit dieser Art von Kriminalität befassen. Oftmals spielen auch Gewalttaten eine Rolle. In einigen Bereichen gibt

es auch Mafiabeteiligungen. Bei einigen Fälschern haben wir auch Schrotgewehre und automatische Waffen gefunden. Einmal hatten wir auch ein Geldwäscheverfahren zu betreuen, in dem wir feststellten, dass Geldwäsche eben auch eine Rolle spielt als Bestandteil dieser organisierten Fälschungsstraftäter. Wir haben einmal in einem Lager riesige Mengen gefälschter Software festgestellt. Wenn man einen solchen Fall hat, dann bedeutet das natürlich auch, dass eine große Menge Geld im Spiel ist. Wir haben durchaus viel Erfolg gehabt. Wir haben Fortschritte gemacht. Hier meine ich natürlich die Gemeinschaft der Strafverfolgungsbehörden.

In den letzten drei Jahren sind die Fallzahlen gestiegen. Das heißt, die Anzahl der sichergestellten gefälschten Produkte ist sprunghaft angestiegen. Der Wert beläuft sich nunmehr auf vier Milliarden Dollar. Wir gehen davon aus, dass noch sehr viel mehr Fälschungsprodukte in Umlauf sind und dies nur die Spitze des Eisbergs ist. Ein weiterer Fall, der sich in Italien und in Singapur abspielte, beinhaltete wahrscheinlich auch eine Mafiaverwicklung. In einem weiteren Fall im Vereinigten Königreich, war eine große Zahl von Bürgern aufgrund eines Raubüberfalls an Zertifikate herangekommen und hatte dann gefälschte Produkte in London herstellt. Die Täter wurden festgenommen und zu drei bis vier Jahren Freiheitsstrafe verurteilt. In einem weiteren Fall war das FBI führend tätig, um einen Fälscherring zu zerschlagen. Viele der Täter gingen arbeitsteilig vor. Die Software wurde in Malaysia hergestellt. Der Vertrieb fand im Vereinigten Königreich statt. Es gab eine Zielperson, die sich in erster Linie mit dem Import befasste. Auf diese Person ist das FBI aufmerksam geworden. Das heißt, das FBI ist nach Europa gekommen und hat sich auch verdeckter Ermittlungsmethoden bedient, um den Täter dingfest zu machen. Eine grenzüberschreitende Zusammenarbeit der Straf- und Strafverfolgungsbehörden ist ebenfalls ein entscheidender Aspekt, wenn wir erfolgreich sein wollen.

Letztes Jahr warf ein Presseartikel die Frage auf, ob die gesetzliche Grundlage überhaupt streng genug ist, um dem Problem der Fälschung von Softwareprodukten Herr zu werden.

Ich möchte jetzt noch einmal auf die Geschichte mit dem Taxifahrer zurückkommen. Vor vier Jahren gab es einen spektakulären Fall hier in Deutschland, wo jemand falsche Software in Deutschland und im Vereinigten Königreich herstellte. Damals wurde eine ganze Fabrik aufgebaut. Ich sagte, dass der Großteil der Fälscherwerkstätten nicht hier in Westeuropa ist. Aber durchaus ein nennenswerter Anteil. Der Täter wurde zu vier Jahren Freiheitsstrafe verurteilt. Aber es wurde kein Pfennig von den illegalen Gewinnen sichergestellt. Wir wissen jedoch, dass der Straftäter riesige Summen auf seine Seite gebracht hatte. Deshalb wurde die Frage aufgeworfen, ob die Gesetze streng genug sind. Meine Antwort ist: Nein! Zum Teil liegt es auch an der Rechtsanwendung. Das ist Teil meiner Botschaft. Deshalb bitte ich Sie alle, noch mal über die Worte des Taxifahrer nachzudenken und sich darüber Gedanken zu machen, wie man an das Geld der Straf-

täter kommt. Man hat zum einen die zivilrechtlichen Verfahren, dann die strafrechtliche Seite eines Verfahrens. Wir haben natürlich Schwierigkeiten, zivilrechtlich an unser Geld zu kommen, wenn die Mittel des Strafrechts schon nicht ausreichend sind. Es ist wichtig, dass man bei großen illegalen Gewinnen auch ein entsprechendes Risiko hat, verfolgt zu werden und tatsächlich eine Haftstrafe zu bekommen. Denn meines Erachtens muss es noch stärker ins Bewusstsein dringen, dass hier wirklich ein großer Schaden angerichtet wird. Ich meine, das Gesetz muss nicht unbedingt härter gemacht, es muss nur besser angepasst werden, um dem Problem Herr zu werden. Wenn Software tatsächlich industriemäßig hergestellt wird, dann ist das eine andere Qualität. In diesem Fall muss man natürlich auch über vermögens-/gewinnabschöpfende Maßnahmen nachdenken.

Ich denke, man hat hier schon sehr viel über die Notwendigkeit einer Zusammenarbeit zwischen privatem Sektor und der öffentlichen Hand gesprochen. Meines Erachtens ist das ein wichtiger Aspekt. Auch bei dieser Form der Zusammenarbeit müssen wir uns Gedanken darüber machen, wie wir an die illegalen Gewinne herankommen. Meines Erachtens hat die Polizei eine hervorragende Arbeit geleistet bei der Festnahme der Täter. Aber man hat sich noch nicht richtig Gedanken darüber gemacht, wie man eben auch an die illegalen Gewinne herankommt. Ich bin sehr froh über das, was in Deutschland kürzlich stattgefunden hat. Wir sehen, dass Deutschland führend ist bei der Bekämpfung von Softwarepiraterie. Wir hatten kürzlich hier einen Fall, bei dem sich die Strafverfolgungsbehörden und die Staatsanwaltschaft sehr hartnäckig auf die Fersen eines Straftäters gesetzt hatten. Diese Person wurde festgenommen. Es wurden zwei Millionen an illegalen Gewinnen auf einem Schweizer Konto festgestellt. Diese illegalen Gewinne wurden eingefroren. Mehrere Millionen Dollar, die nach Ägypten und aus Ägypten heraus transferiert wurden, wurden als Kaution hinterlegt. Und das Geld wurde von Ägypten nach Deutschland transferiert. Der Verteidiger hat dieses Geld illegal gewaschen und dazu benutzt, seinen Mandanten wieder auf freien Fuß zu bekommen. Wir müssen sicherstellen, dass das Strafmaß angemessen ist und dass es wirklich dem Ausmaß des Schadens Rechnung trägt.

Ich möchte auf einen weiteren Fall zu sprechen kommen, den die Menschen hier sicherlich auch kennen. Es ging damals um viele Täter in verschiedenen Bundesländern der Bundesrepublik. Es wurden umfangreiche Erkenntnisse gesammelt, es gab diverse Verfahren, verteilt über Deutschland, die eröffnet, dann wieder eingestellt wurden. Das BKA hat hier eine herausragende Rolle gespielt. Es hat die einzelnen Verfahren zusammengeführt, hat eine Koordinierungsfunktion wahrgenommen. Das zeigt, wie wichtig es ist, eine nationale Zentralstelle zu haben, die Fälle koordiniert, und die einen Gesamtüberblick hat über das, was in Deutschland passiert. Bis jetzt sind einige Personen festgenommen worden. Das BKA hat sich tatsächlich um die illegalen Gewinne in diesem Verfahren gekümmert, bei dem fünf Täter festgenommen wurden – bis jetzt. Nach Ihrer Definition hat OK damit zu tun, dass die Täter ihre Gewinne im Vorfeld ausgerechnet haben, dass also sehr viel Planungsarbeit eine Rolle spielt. Wir hatten es hier

durchaus mit einem Fall schwerer Kriminalität zu tun. Es gab mehrere Personen, die arbeitsteilig vorgegangen sind. Es gab Gewinnstreben, es gab Arbeitsteilung. Der Aspekt der Abschottung spielte eine Rolle, so dass hier alle Merkmale der Organisierten Kriminalität vorlagen. Und es wurde über eine längere Zeit zusammengearbeitet, so dass es, wie gesagt, ein typischer OK-Fall war.

Es war ein hervorragendes Verfahren und ich weise auf die hervorragende Rolle des BKA hin. In einer Presseveröffentlichung des BKA wird darauf hingewiesen, dass es ein wichtiges operationelles Spiel ist, das Vermögen des Täters aufzudecken und es in erster Linie darauf ankommt, illegale Gewinne sicherzustellen und hier den Verfall anzuordnen. Ich glaube, dass wir hier sehr große Fortschritte gemacht haben. In dieser Hinsicht sollte dem BKA nachgeeifert werden und das Beispiel des BKA auch in anderen Bereichen verwirklicht werden.

Eine weitere Herausforderung, auf die ich eingehen möchte, bezieht sich auf die Sicherheit des Internets. In früheren Vorträgen ist bereits von „Würmern" die Rede gewesen. Wir sind zunehmend Angriffen von Hackern ausgesetzt. Es wird sehr viel Aufmerksamkeit auf präventive Anstrengungen gerichtet. Die Frage ist: Wie kann man die Infrastruktur sicher machen? Wie kann man sein Computersystem abschotten und sicher machen gegen solche Hacking-Angriffe? Das ist das, worum sich viele Leute kümmern, auch viele Hunderte, Tausende von Mitarbeitern bei Microsoft, die entsprechende Strategien und Software entwickeln. Aber es gibt noch einen anderen Aspekt. Das ist die Festnahme, das heißt die Verantwortung der Täter vor Gericht. Sie müssen vor Gericht gebracht werden. Die, die solche Hacking-Angriffe durchführen, solche „Würmer" und „Trojaner" etc. verbreiten. Denn die Schäden sind enorm. Im Jahr 2003 belief sich der Schaden, der verursacht wurde, auf 13.000.000.000 Dollar. Die Kosten, um sich vor Viren zu schützen, belaufen sich auf 3,8 Milliarden pro Jahr.

Aber wir müssen über diese Zahlen hinausschauen. Man muss daran denken, dass viele Personen versuchen, Einkäufe über das Internet zu tätigen. Da ist es natürlich fatal, wenn Straftäter persönliche Daten ausspionieren und sich die Daten zu Eigen machen und das für enorme illegale Gewinne benutzen. Ich bin schon von Freunden angerufen worden, die sagten, sie haben zwei Tage frei, weil ihr Computersystem lahm gelegt sei und sie daher nicht arbeiten können. Man muss bedenken, dass bestimmte Viren, bestimmte Angriffe, sehr schnell Wirkung zeigen. Es gab einen Fall, in dem ein Wurm eine Rolle bei der Schädigung einer Nuklearfabrik gespielt hat. Sehr oft kommt es vor, dass sich Leute entschuldigen und sagen: „Tut mir leid Chef. Mein Computersystem ist lahm gelegt." Man kann sich vorstellen, dass das fatal ist, wenn so etwas in einem Krankenhaus oder in einer anderen kritischen Einrichtung vorkommt.

Viele Beschuldigte sind natürlich darauf aus, Geld zu machen. Es geht darum, zu stehlen, Profite zu machen. Aber es gibt auch andere Motive. Dazu gehört beispielsweise einfach das Verursachen von Schaden, einfach nur um des Schadens willen. Manchmal geht es auch darum, sich einfach nur einen Namen zu machen

in der Gemeinschaft der Hacker. Da geht es letzten Endes nur darum, sein eigenes Ego zu befriedigen. Meines Erachtens gibt es überhaupt keinen sinnvollen Nutzen solcher Tätigkeit.

Die führende Rolle muss von den Strafverfolgungsbehörden übernommen werden. Als Vertreter der Industrie können wir letzten Endes nur eine unterstützende Rolle einnehmen. Wir können unsere technischen Ressourcen bereitstellen, um dazu beizutragen, dass die Strafverfolgungsbehörden erfolgreich sind und Täter dingfest machen können. In einer Welt, in der die Hacker irgendwo abgeschottet arbeiten, wo man sie nicht sehen kann, ist es natürlich sehr schwer, ihrer habhaft zu werden. Sie hinterlassen keine Fingerabdrücke wie Allgemeinkriminelle. Es gibt natürlich gewisse Spuren. Aber es gibt für die Hacker auch Möglichkeiten, ihre Spuren wieder zu verschleiern. Und es gibt keine Zeugen im klassischen Sinn. Es gibt keine Augenzeugen, wie wir sie aus dem allgemeinkriminellen Bereich kennen. Natürlich arbeiten solche Täter auch grenzüberschreitend. Das heißt, eine Grenze bedeutet für einen Hacker gar nichts. Die kann er locker überschreiten. Das ist auch ein Phänomen, dessen sich die Strafverfolgungsgemeinschaft bewusst sein muss. Die Hacker müssen auch schlafen. Sie haben ein reales Leben. Die Herausforderung für uns ist es, sie aufzuspüren, sie in ihrer realen Welt aufzuspüren, sie dingfest zu machen und vor Gericht zu bringen.

Wir wissen, dass große Anstrengungen vom BKA unternommen wurden, dass das BKA weltweit aktiv gewesen ist und dass man sich dieser Aufgabe erfolgreich stellen kann. Es gab kürzlich ein Programm von FBI und Secret Service, das das Ziel verfolgt, entsprechende Erfolge auch zu würdigen. Das heißt, wir bezahlen Leute, die uns Informationen bereitstellen über Personen, die in Systeme eindringen, die Viren verbreiten. Wir haben mit dem Secret Service und dem FBI auch in vielen Bereichen zusammengearbeitet. Und wir haben dieses Belohnungssystem von Microsoft bereits erfolgreich eingesetzt. Die Strafverfolgungsbehörden müssen eine führende Rolle übernehmen. Es ist bereits sehr gute Arbeit geleistet worden. Ich möchte Sie dazu aufrufen, sich dieser Herausforderung zu stellen und weiter den begonnenen Weg erfolgreich zu beschreiten.

Zukunftsperspektiven: Wirtschaftliche Entwicklung und IT-Sicherheit

Klaus Brunnstein

Einleitung

Indem ich mich herzlich für die Einladung zu Ihrer Tagung bedanke, möchte ich anmerken, dass ich die Einladung in einer Situation bekam, die mir zu denken gab. Ich hatte kurz vorher für ein Jugend-Strafverfahren ein Gutachten zu erstellen im Fall eines Jugendlichen, der sich IT-Methoden (Email, Webmail) zunutzte machte, um andere Schüler mit Gewalt zu bedrohen („Morgen rummst es gewaltig, da ist Erfurt gar nichts dagegen gewesen"). Dabei fand ich die Asservate, die mir von den Aufklärungsbehörden übergeben wurden, eigentlich nicht auf dem Stand vor, den ich schon vor über zehn Jahren in der forensischen Informatik gelehrt hatte.

Bereits Mitte der 90er Jahre haben zwei meiner Diplom-Studenten für das Bundeskriminalamt eine Software zur forensischen Aufklärung von Datenträgerinhalten entwickelt (Michael Reinschmied, Jörg Steindecker: „Konzept einer Skriptsprache zur Analyse von Strukturen auf Datenträgern (Ein Beitrag zur forensischen Informatik)". Dieses Programmsystem ist auch eine Zeitlang erprobt worden und wurde dann auch bei einigen Landeskriminalämtern eingesetzt. Weil damals keine Chancen für eine Weiterführung des Projektes bestanden, ist einer dieser Studenten zur australischen Polizei ausgewandert, der andere wurde IT-Sicherheitsbeauftragter einer sehr großen Versicherung.

Auch wenn dieses Beispiel nur zeitweilig erfolgreich war, sehe ich in einer partnerschaftlichen Zusammenarbeit von Informatik und Strafaufklärung eine wichtige Aufgabe. Es hat ja auch Tradition, dass die Kriminalpolizei, insbesondere das BKA mit Kriminologen z. B. der Universität Frankfurt regen Kontakt hat und von der Zusammenarbeit profitiert. Ich rate daher, dass dieses auch mit den forensischen Informatikern – obwohl es bisher nur wenige gibt – in den Landeskriminalämtern zu einer spürbaren Verbesserung der Arbeit führt. Ich erinnere mich noch, wie ich damals beim „KGB-Hack" dem BKA in Meckenheim helfen konnte, die vorgefundenen Datenträgerinhalte aufzuklären. Unter diesen Umständen ist mein Beitrag hier auch ein Werben für eine Partnerschaft mit Wissenschaft und Universitäten, insbesondere auch bei der Ausbildung von Polizisten. Ich weiß allerdings, dass hier gewisse Hürden bestehen, zumal die Wissenschaft der Offenheit gewidmet ist und dies nicht immer die Aufgabe einer Strafverfolgungs- oder auch Aufklärungsbehörde sein kann.

Nach dieser kurzen Vorbemerkung leite ich meinen Vortrag mit einer Übersicht ein. Ich werde etwas über die technisch getriebenen Entwicklungen der Informationswirtschaft sagen. Sie wissen vielleicht, dass in der nächsten Woche der UNO-

Gipfel („World Summit on the Information Society“) in Genf stattfindet, in der ein wichtiger Aspekt die Überwindung der so genannten „digitalen Lücke“ (Digital Gap) zwischen den Entwicklungs- und den entwickelten Ländern ist. Dabei wird auch die Diskussion geführt, wie in Zukunft die Informations- und Kommunikationstechnologien die Gesellschaften rechtlich, organisatorisch, kommerziell sowie im Privatbereich formen werden. Hierzu werde ich eine historische Analogie bringen, die auch einige Risiken der heutigen Informationstechnik beleuchtet. Das Fazit meines Vortrages im zweiten Teil wird leider sein: Die heutige Technik ist inhärent, also in ihrem Kern, unsicher und riskant, und um uns zu schützen müssen wir neue Methoden entwickeln. Auf absehbare Zeit werden unliebsame Vorfälle – etwa Verbreitung von Viren und Würmern – und auch krimineller Missbrauch durch die Technik begünstigt. Es wird auch sehr schwer sein, kriminellen Missbrauch aufzuklären. Aber es gibt einige Ansätze, die ich ganz zum Schluss noch bringen werde. Dieses ist der Bogen, den ich spanne.

Prof. Dr. Klaus Brunnstein von der Universität Hamburg äußerte sich besorgt über die Zukunft der IT-Sicherheit

Die Industriegesellschaft: Muster einer technisch geprägten Gesellschaft

Meine Damen und Herren, zunächst also die historische Analogie. Bekanntlich hat Technik die menschlichen Produktions- und Lebensformen seit langem beeinflusst, auch im Altertum und schon davor. So haben die Erfindungen des Rades, der Verkehrswege, der Schiffe seit alters her menschliche Gesellschaften geprägt.

Aber eigentlich hat das von Technik geprägte Wirtschaften erst mit der Erfindung der doppelt-wirkenden Niederdruck-Dampfmaschine 1762 des James Watt richtig begonnen. Erst damals entstehen mit anfangs noch sehr schweren, eher leistungsschwachen Maschinen die industriellen Produktionsfaktoren, in denen Rohstoffe der materiellen Welt mithilfe von Maschinen zu immer komplexeren Produkten „veredelt" werden, auch zu Maschinen, mit denen noch komplexere Produkte hergestellt werden können. Dieser Prozess, der übrigens erstaunliche Ähnlichkeit mit der Entwicklung der Informationstechnik hat, dauert etwa fünfzig Jahre (das werden erst im 20. Jahrhundert der österreichische Nationalökonom Schumpeter und der russische Mathematiker Kondratieff in ihren Zyklentheorien herausfinden), in denen die Maschinen schrittweise immer leistungsfähiger wurden, so dass am Ende dieser ersten Epoche der Industriegesellschaft – etwa um 1810 – man sie auf einen sich bewegenden Wagen setzen und damit vom Orte bewegen konnte („Lokomotion"), sodass nunmehr massenhaft Rohstoffe für die industrielle Produktion von entfernten Orten an die Stelle der Produktion herantransportiert und die Veredelungsprodukte zu ihren Einsatzorten transportiert werden konnten. So stürmisch die Entwicklung des Eisenbahnnetzes auch geht, diese Entwicklung dominiert die zweite Phase wiederum grob etwa 50 Jahre.

Hier sind zwei Aspekte interessant, die ähnlich bei der Informations- und Kommunikationsgesellschaft zu beobachten sind: in der Anfangsphase wird die Innovation von schweren, leistungsschwachen und lokal arbeitenden Maschinen voran getrieben, die schrittweise immer leistungsfähiger wurden. In der zweiten Phase dominiert dann die ortsbewegliche Maschine als Grundlage des Transports von Gütern und Menschen, und diese erweitert den lokalen Einsatz in regionale, teilweise auch globalisierte Bereiche. Schon damals gab es Managementverfahren, wenn auch weitgehend manuell, etwa in der Akquisiton und Abrechnung von Lieferungen. Zwei weitere Phasen der Industriegesellschaft werden von anderen Maschinentypen (getrieben von Erdölderivaten und elektrischer Energie) bestimmt, aber diese 3. und 4. Phase der Industriegesellschaft – obwohl wichtig durch die Entwicklung von Telefon und Elektrizität als Voraussetzung für die heutigen I&K-Techniken – helfen nicht bei der Betrachtung der Anfangsphasen der Informationsgesellschaft und werden daher hier nicht weiter betrachtet.

Die Informationsgesellschaft: Analogien und neuartige Entwicklungen

In der heutigen Entwicklung, die sich analog in zwei Phasen aufteilen lässt, finden wir, dass die Industrie immer kleinere Teile der Wertschöpfung in der Welt einnimmt. Natürlich ist das nach Sektoren und nach Weltregionen unterschiedlich. Aber andere Dinge, wie zum Beispiel technikgestützte Wertschöpfung, virtueller Handel wie etwa E-Commerce gewinnen an Bedeutung und tragen zum Bruttosozialprodukt erheblich mehr bei.

Natürlich werden industrielle Produkte und Verfahren auch in dieser postindustriellen Industrie gebraucht, so wie es auch in den vorigen und jetzigen Phasen agrikulturelle Produktionen gibt, wenn auch mit schwindendem Anteil an der Wertschöpfung. Neu hinzu kommen in der I&K-unterstützten Welt, dass Organisationen einen von Ort und Zeit abgelösten Charakter bekommen, dass sie „virtuell" werden. Man kann heute ein Unternehmen von der Jacht aus der Karibik weltweit führen, indem man lokale Verarbeitungs- und Speicherungseigenschaften über weltweite Netze nutzt. Damit ändern sich die Rahmenbedingungen gegenüber den 200 Jahren der Industriegesellschaft grundlegend.

Ein weiterer Aspekt der Industriegesellschaft betrifft Fragen wie: Wer treibt denn die Entwicklung der Gesellschaft? Welche Auswirkungen auf Sicherheitsaspekte hat das? Beide – Industriegesellschaft wie Informationsgesellschaft – werden von der Anbieterseite gestaltet, sie sind Formen einer Supply Side Economy, die von Erfindern und Technologieanbietern bestimmt werden. Nicht die Nachfrageseite, nicht der sprichwörtliche Markt bestimmt, welche Funktionen die Mobiltelefone, die Laptops oder die Software haben. Es ist also kein Markt in dem Sinne, dass die Kunden bestimmen, was geliefert wird, sondern die Hersteller bieten etwas an und die Kunden haben nur die Wahl, es zu nehmen oder nicht. Dies hat sowohl in der Industriegesellschaft wie in der Informationsgesellschaft zu monopol- oder doch oligopol-artigen Strukturen geführt. Wenn Sie sich die Wirtschaftsmacht der ersten Phasen der Informationsgesellschaft ansehen, so war IBM (neben anderen wie Telefunken, die später verschwanden) mit den Mainframes ebenso bestimmend wie heute Microsoft bei den PCs. Offenbar nur mit solchen Oligopolen war es möglich, anfangs diese riesengroßen Rechner und ihre Applikationen überhaupt so weit zu bringen, dass sie in der Wirtschaft einsetzbar waren. Diese sind dann immer kleiner und stärker geworden, aber ihre Verbreitung hat ebenfalls ein Monopol begünstigt.

Mit Unterstützung von IBM (die Bill Gates das Monopol auf das DOS-Betriebssystem schufen) ist dann Microsoft entstanden. Damals wurde die Idee des „Personal Computers" (PC) propagiert, nämlich eines in der Leistung abgespeckten Computers, über den man sozusagen „persönlich" die Herrschaft haben konnte. Damit konnte man arbeiten, hatte aber eine Leistung, die natürlich nicht vergleichbar war den Großrechnern. Erst in einer späteren Phase ist Microsoft vermittels der Emanzipation der kleinen über die großen Geräte und des Anschlusses an die Netze in die Situation gekommen, IBM abzulösen und heute mit rund 90 % Marktanteil – wie früher IBM bei den Mainframes – den Markt zu dominieren. Ähnliches galt auch schon in der Industrieentwicklung von England („Manchester-Kapitalismus") über das Ruhrgebiet (Krupp) bis in die US-Wirtschaft (Bahnbarone). Solche Monopole, die sich später auflösen, könnten somit der Preis für die Verbreitung einer komplexen und teuren Technologie sein.

Ein interessanter Aspekt der Entwicklung betrifft auch die Sicherheitstechnik. So hat es jeweils etwa 80 bis 90 Jahre gebraucht, bis sich eine Sicherheit industrieller

Verfahren und Techniken entwickelte. In der ersten Phase nach James Watt waren Unglücke mit Dampfkesseln sowohl in Fabriken wie bei den ersten Eisenbahnen an der Tagesordnung. Als die Dampfkesselhersteller merkten, dass dies ihren Markt beeinträchtigte, gründeten sie den „Dampfkessel-Ürwachungsverein", Vorläufer des heutigen TÜVs. Dieser Verein war ein Versuch der Hersteller von industriellen Produkten, die Qualität anzuheben und damit die Risiken dieser Technik in den Griff zu bekommen. Es hat etwa 60–70 Jahre nach James Watt gedauert, bis dieses Risikobewusstsein sich entwickelte. Interessant ist, dass etwa dasselbe heute passiert, etwa 60 Jahre, nachdem die ersten Computer laufen lernten, wobei ich als Startjahr 1941 in Berlin, nämlich den Bau der Z 3 des Konrad Zuse (Ehrendoktor meines Hamburger Fachbereichs) annehme.

Etwa 60 Jahre nach der Erfindung des Computers haben wir derart schwerwiegende Vorfälle, dass man an die Unsicherheitsprobleme herangehen muss. Dasselbe ist übrigens in der dritten und vierten Phase der Informationsgesellschaft ebenfalls passiert, als nämlich die Autos erfunden wurden. Bis 1950 etwa, als das Auto in den Vereinigten Staaten schon ein Massenverkehrsmittel war, gab es erhebliche Produktionsmängel, wodurch Passanten und Insassen fabrikneuer Autos verletzt oder getötet wurden. Damals schrieb ein junger Jurist, Ralf Nader, eine Doktorarbeit: „Unsafe at any speed". Wenn man sich heute ansieht, wie rasend schnell die Mikroprozessoren geworden sind, so dass keiner von uns „mit dem Denken mitkommt" (abgesehen davon, dass wir gar nicht so denken wie diese Chips mit Befehlen wie Laden, Speichern etc. Arbeiten), dann ist das Wort „Unsafe at any speed" für die Informationsgesellschaft mindestens so relevant wie sie in den fünfziger Jahren für die Entwicklung des Verbraucherschutzes in den Vereinigten Staaten war.

Neuartige Beziehungsgeflechte in der Informationsgesellschaft

Man kann für die Entwicklung der Informationsgesellschaft einiges aus der Industriegeschichte lernen, vor allem über Risiken. Die Entwicklungen verlaufen in Zyklen, heute nach Kondratieff als Kondratieff-Zyklen bekannt. Dabei wird eine neue Idee wachsen, sich verbreiten, reifen, bis auf der nächsten Ebene die nächste Technikgeneration kommt. Diese Zyklen dauern etwa 40 bis 45 Jahre. Wir stehen jetzt in der zweiten Phase, und wir fangen nun an zu sehen, dass sich vieles, wenn nicht alles ändert. Wenn wir bisher die Beziehungen als Kunde, Staatsbürger, Student betrachten, waren das physische Beziehungen, über die wir Vertrauen etwa zu dem Hersteller eines Produktes, zum Händler eines Produktes, zu unserer Bank, zu unserem Lehrer, aufgebaut haben.

Alle diese Beziehungen werden nun „virtuell". Die Beziehungen zwischen Patienten, Arzt, Krankenhaus oder Krankenkasse werden abgebildet auf E-Relations. Die Beziehung von Studierenden als Lernende zur Universität wird abgebildet auf E-Learning. Die Beziehung eines Kunden zum Handel wird abgebildet auf E-Commerce, zur Bank auf E-Banking, als Bürger auf E-Voting, E-Govern-

ments, E-Steuerzahler, und so weiter. Das Vertrauen, das wir früher durch persönliche Kontakte aufgebaut haben, müssen wir nun aufbauen zu Systemen, die wir nicht mehr in der Lage sind zu durchschauen. Wenn wir im Internet eine Recherche machen, müssen wir uns darauf verlassen, dass die Information, die wir bekommen, die Antwort auf unsere Frage ist und nicht eine Verdrehung der Tatsachen. Wir müssen davon ausgehen, dass, wenn wir ein System brauchen, dieses uns zur Verfügung steht, dass auch niemand anderes dieses System irgendwo unterlaufen kann, dass man uns zum Beispiel kein X für ein U vormacht, indem man eine vermeintliche E-Mail von unserer Personalabteilung bekommt: „Kommen Sie morgen ins Personalbüro. Wir möchten mit Ihnen ein Gespräch führen." Das heißt: Wir bauen unser Vertrauen auf Technologien auf, die wir im Prinzip nicht kontrollieren können. Das ist der Unterschied zur Industriegesellschaft, denn dort waren die Rohstoffe, die Maschinen und die Güter materielle Güter.

Selbst wenn wir in unserem Mercedes auf einer herbstlichen Landstraße mit zu hoher Geschwindigkeit fahren, merken wir körperlich, wenn dieses System ausbricht. Wir haben noch eine physische Erfahrung. Aber diese physische Erfahrung haben wir nicht mit dieser Art von virtuellen Systemen, die nicht mehr durchschaubar sind. Und es wird noch interessanter. Ein Teil dieser Verbindungen stellt das Internet her. Viele meinen: das internet ist die Hoffnung, ist die Zukunft! Meine Damen und Herren, ich muss sagen: das Internet ist Risiko. Das Internet wurde nämlich nicht für vertrauenswürdige Kommunikation geschaffen, sondern es wurde von Wissenschaftlern mit Geld der amerikanischen Regierung geschaffen, damit man zwischen Forschungsinstitutionen schnell kommunizieren konnte. Von Schutzbedarf keinerlei Ansatz. Aber natürlich gibt es schutzbedürftige Bereiche wie zum Beispiel die inneren Netze von Unternehmen, Dienststellen wie dem BKA: wie wir heute sagen, den Intranets. Es besteht also ein Schutzbedarf, aber die heutigen Techniken unterstützen dies gar nicht. Doch dazu später.

Zur Vernetzung der Chip- und Computerwelten

Meine Damen und Herren, wir haben heute bei einer Größenordnung von 50 bis 100 Millionen Servern (also Dienst- und Verbindungsrechnern) etwa 600 bis 700 Millionen Arbeitsplätze (Clients) im Internet. Rechnen wir mal hoch: mit 100 Millionen Server im Jahr 2007, die die Dienste im Internet bringen, werden etwa 1.000 Millionen User „am Internet hängen". Doch jetzt kommt eine Entwicklung, die das Netz ganz erheblich verändern wird, nämlich die so genannten „intelligenten eingebetteten Geräte" (smart embedded devices). Ein Beispiel dafür sind die „persönlichen digitalen Assistenten" (PDAs), in denen man seinen Zeitplan, seine Telefonnummern und Notizen abspeichern und heute auch schon telefonieren und Email versenden kann.

Diese Geräte können mit vielen Geräten des täglichen Lebens, etwa in Auto und Haushalt kommunizieren. Hier ein Beispiel aus einer Diskussion bei Daimler Chrysler: nach einem harten Tag kommen Sie nach Hause, wo Sie eine Reihe

von Freunden zu einer schönen Party eingeladen haben. Sie nähern sich Ihrem Auto. Der Transponder, den Sie in Ihrer Kleidung tragen, identifiziert sie zuverlässig als berechtigter Fahrer des Autos.

Nebenbemerkung: *Die Chips, die wir an unseren Kleidern tragen etwa als Identifikatoren – eine Idee die schon vor zehn Jahren am berühmten MIT (Massuchesetts Institute of Technology, Boston) erdacht wurde – nennen wir „WearWare" (grob übersetzt: am Körper getragene Chips, denn wir tragen die Computer als Teil bei uns). Einige von diesen WearWares können sogar in unsere Körper integriert sein, etwa als Hörhilfen im Ohr. Die Leistungen dieser Chips sind noch längst nicht ausgeschöpft. Zum Beispiel könnten sie die zur persönlichen, vielleicht auch besseren Kommunikation in das Ohr hinein benutzen, etwa zur Übersetzung. Es gibt eine Vielzahl solcher Beispiele möglicher Anwendungen.*

Aber nun weiter im Beispiel. Ihr Car-Management-System (CMS) in Ihrem Auto startet schon ihren Wagen oder wärmt Ihren Sitz vor. Nun aber wird ihr „persönlicher digitaler Assistent" sich mit Ihrem Haushaltssystem (Household Management System, HMS), welcher Ihren Kühlschrank und Weinkeller verwaltet, in Verbindung setzen – natürlich über Funk-Internet – und anfragen: „Fehlt noch was?" Woraufhin Ihr Haushaltssystem mitteilt: „Roter Wein, Käse, alles da. Aber dieses schöne grüne Kraut, was du immer mit deinen Freunden rauchst . . . . . " – Aber ich glaube, das Beispiel darf ich hier nicht bringen. Also: irgendwas fehlt. Daraufhin antwortet das Car-Management-System: „Dies muss unterwegs besorgt werden. Bloß auf dem Wege zu dem Händler ist Stau, da muss ich sowieso einen Umweg fahren. Dann hole ich auch gleich diese interessante Hackerzeitschrift, die mir die neuesten Sachen über Hacker-Attacken zur Nachahmung bringt."

Meine Damen und Herren, in Ihrem Auto sind heute rund 30 Chips, wenn Sie ein Spitzenklassemodell der letzten Generation besitzen – und in der nächsten Generation sind 50 bis 100 Chips drin, die wichtige Aufgaben erledigen. Und immer wenn etwas nicht funktioniert, fahren Sie in die Werkstatt oder werden dorthin abgeschleppt. Das Erste, was man dort macht, ist nicht eine Diagnose, sondern es werden alle Fehlerbits gelöscht. Dann können Sie weiterfahren. Soweit zur Zuverlässigkeit der heutigen Technologie. Und die Zahl der „eingebetteten Chips" steigt ständig weiter, und die Verbindungen zum Internet ebenso. Bei der Lufthansa haben Sie bei den Transatlantik-Flügen schon heute einen Internet-Anschluss.

Zur Risikoanalyse heutiger Informationstechniken

Meine Damen und Herren, leider sind wir noch nicht im Jahr 70 der Informationsgesellschaft, in der die IT-Hersteller so klug sein könnten wie die Dampfkesselhersteller, einen IT-Überwachungsverein aufzumachen (die heutigen TÜVs bemühen sich zwar redlich, aber ihre Mission ist eben an der Industriegesellschaft

ausgerichtet, ihre Methoden für die I&K-Gesellschaft ungeeignet). Deshalb will ich kurz analysieren, an welcher Stelle diese Technologie wesentliche Risiken hat. Man kann diese Risiken – die sich in Softwareabstürzen, Hackerangriffen und IT-Kriminalität äußert – nicht alleine (ja nicht einmal primär) den pubertierenden männlichen Jugendlichen zwischen 15 und 50, die Viren schreiben und Hacker-Angriffe durchführen, zur Last legen. Vielmehr sind diejenigen verantwortlich, die diese Technik wissentlich mit schweren Mängeln produzieren und vertreiben.

Erstens: Wir haben eine ganze Reihe hausgemachter Risiken, insbesondere überhöhte Komplexität und die Forderung nach Zusammenarbeit einzelner Systeme (auch und gerade, wenn diese bereits zu komplex sind). Zweitens: Wir haben eine Menge von Fehlern in den Entwürfen der Systeme, etwa weil Sicherheitsforderungen überhaupt nicht berücksichtigt sind. Drittens gibt es erhebliche Probleme bei der Softwarefertigung. Und viertens sind die Benutzer, die selbst oft „auf Gedeih und Verderb" auf diese Techniken angewiesen sind, selbst ein erhebliches Risikopotential (weshalb man die „User" in Sicherheitskreisen gern als „Looser" bezeichnet).

Die Schichten der Systeme, von der Präsentation über die Betriebssysteme, die Firmensoftware bis zur Hardware ist heute mehrere Gigabyte dick. Die Schichten sind so dick, dass man als Anwender gar nicht mehr durchblicken kann. Selbst der Sicherheitsexperte, der viele Unfälle untersucht, wird ja nur gerufen, wenn irgendwo wieder ein Virus sein Unwesen treibt oder irgendetwas anderes nicht funktioniert; dann soll er sich diese dicken Schichten angucken und sagen, was in der Tiefe des Systems passiert. Das ist, als ob Sie versuchen, sozusagen von der Oberfläche des Ozeans in 8.000 Meter Tiefe zu schauen: mission impossible! Die Komplexität aber ist etwas, das die Verbraucher nicht zu vertreten haben. Wenn Verbraucher wählen könnten, würden sie sagen: „Ich möchte gerne eine Software, die einfach ist und funktioniert." Hacker-Angriffe interessieren da nicht: sie soll funktionieren und nicht dauernd zusammenbrechen.

Meine Damen und Herren, ich entschuldige mich bei meinem Vorredner David Finn von Microsoft. Es könnte so aussehen, also ob ich hier eine Anti-Microsoft-Rede hielte. Das ist nicht der Fall. Alle Technologien sind unsicher, ob sie LINUX nehmen, das heute vom Deutschen Bundestag und einigen Bundesländern und Städten favorisiert wird, oder ob sie Microsoft nehmen. Die Systeme bauen alle auf derselben technologischen Basis auf. Die Leute haben alle dieselbe Art von Hardware, von Programmierung usw. gelernt: C-Programmierer, Basic-Programmierer, wie auch immer. Keine Vorstellung von Sicherheit allenthalben, die im Entwurf berücksichtigt sein muss, keine Ausbildung zur Herstellung sicherer Software. Ich habe mal die Nachrichten von einem Jahr über die wirklich gravierenden Vorfälle zusammengestellt. Danach hat es von Oktober 2002 bis heute etwa 15.000 (!) Fehlermeldungen gegeben, davon rund 100 zu Microsoftsystemen. Wenn man nur die allerwichtigsten nimmt, betreffen 90 % der Vorfälle Systeme von Microsoft, weil Microsoftsysteme die verbreitetsten und am meisten an-

gegriffenen sind. Die anderen Vorfälle betreffen alle LINUX- und UNIX-Versionen, die in der Wirtschaft ebenfalls, wenn auch weniger verbreitet, eingesetzt werden. Es ist nicht so, dass bei LINUX alles besser wäre.

Viele Leute meinen: Probleme mit Microsoft lösen wir dadurch, dass wir zu LINUX gehen. Ich sage Ihnen voraus: Hätten wir so viel LINUX-Systeme wie Microsoft-Systeme, dann hätten wir zehnmal mehr Viren als heute. Die Anzahl der Viren wird Sie schockieren: es sind über 50.000. Dieses kommt aber nicht so sehr, weil Microsoft viel schlechter ist als alle anderen, sondern weil sie viel angreifbarer sind, da sie die Spitzenposition haben. Klar, alle diese Systeme sind schwach und angreifbar.

Einer der kritischsten Viren war der so genannte SQL-Virus. Hier muss ich leider sagen, dass das auch ein Trauerspiel für die Nutzung von Sicherheitstechnologien bei Microsoft war. SQL ist ein Datenbanksystem von Microsoft. Dort wusste man viele Monate, dass in diesem SQL-System ein schwerer Programmierfehler war. Eine Fehlerkorrektur („patch" genannt) war lange bekannt, als im Herbst 2002 ein Angreifer die Lücke ausnutzte, um einen Virus zu verteilen. Das wäre nicht weiter schlimm, wenn nicht folgendes passiert wäre: der Microsoft-SQL-Server, der alle Fehlerkorrekturen, also auch diesen Patch speichert und verteilt, lief selbst unter dem unkorrigierten System. Das Ergebnis war, dass dieser Server bei den SQL-Wurmangriffen als erstes ausfiel. Man konnte also die vorhandene Fehlerkorrektur von Microsoft nicht herunterladen. Da muss man Microsoft in der Tat einen Vorwurf machen. Immerhin hatte Microsoft etwa sieben Monate bevor dieser Virus die Lücke ausnutzte, alle darauf hingewiesen, dass da eine schwere Lücke existiert, die korrigiert werden soll. Insofern ist das ein Punkt, wo David Finn auch Recht hatte, als er sowie Dr. Helmbrecht vom BSI sagten: man muss die Patches auch einspielen, wenn man die Nachricht bekommt.

Kommen wir zu den durch Medienberichte so bekannten (um nicht zu sagen: aufgebauschten) Würmern der SoBig-Generation. Meine Damen und Herren, bei einem einzigen Internet-Dienstleister sind an einem Tag 100.000.000 SoBig-Würmer über das Netz gegangen. Jetzt werden Sie sagen: 100.000.000 verseuchte Emails ist ja schrecklich. Aber in Relation zu den etwa 2 ½ bis 3 Milliarden – wir wissen das nicht so genau – E-Mails, die pro Tag verschickt werden zwischen Universitäten, Privatleuten oder Wirtschaft: da sind dann 100 Millionen verseuchte Emails eben „nur" 5 % der Netzlast. Trotzdem: Die Presse (nach dem Motto: „bad news is good news") war voll davon. Der Vorteil war, dass alle Leute verstanden: ich muss mein Antivirusprogramm auf den neuesten Stand bringen.

Ein letztes Beispiel für die zunehmende Abhängigkeit und Verletzlichkeit der I&K-Techniken: Der Aufruf von Funktionen durch Fernsteuerung (technisch: remote procedure call, RPC). Mit dieser Technik kann man von seinem Computer die Steuerung über einen anderen Computer übernehmen. Diese Mechanismen werden zum Beispiel benutzt, um Sicherheitskorrekturen einzuspielen. Beispiel: Microsoft bietet eine Fehlerkorrektur an, lädt sie auf ihr System und startet die

Installation der Korrektur. Leider trifft es oft zu, dass Fehlerkorrekturen unzureichend oder sogar schädlich sind, danach sind Korrekturen der Korrekturen fällig und so weiter, ein Teufelskreis.

Sind schon die komplexen Systeme schwer durchschaubar und voller eingebauter Risiken, so vergrößert die Forderung nach Zusammenarbeit (Interoperabilität) die Probleme noch mehr. Gern werden in Unternehmen hochgradig inkompatible Systeme verbunden, zum Beispiel eine Datenbank von IBM, ein Betriebssystem von Microsoft mit einer Anwendungssoftware von SAP. Da diese Systeme nicht aufeinander abgestimmt sind, muss man sie mit einer Art Kaugummi oder Klebeware (glueware) verbinden. Dieses Kaugummi bilden so genannte Skript-Programmiersprachen, mit denen man alles programmieren kann, also neben der „Goodware" – welche die Verbindung zwischen den Systemen herstellt – eben auch „Badware" oder „Malware". Kein Wunder, dass dies die Sprachen sind, mit denen „Skript-Kiddies" sich ein teuflisches Vergnügen machen, wenn sie ihre Angriffe und Würmer schreiben.

Und wie gesagt: das Internet ist Risiko in Reinkultur. Mit dem Internetprotokoll kann man Ihnen beliebig ein X für ein U vormachen. Damit haben Täuschungshandlungen – etwa über Absender und Inhalte – mit minimalen Mitteln leichten Erfolg. Auch die Verweigerung von Diensten („Denial of Service" Attacken) sind so einfach, dass ein 15-jähriger kanadischer Lehrling mit Spitznamen „Mafiaboy" vorgefertigte kleine Programme an verschiedenen Stellen des Internet schlafen legen konnte (daher werden diese Angriffsprogramme auch „Zombies" genannt), sie aufweckte und zu einem Angriff auf den Internetbuchhändler Amazon benutzte. Wohlgemerkt: ein 15-jähriger Lehrling, der keine Ahnung von Programmierung hatte und der nur vorgefertigte Programme benutzte. Jetzt kann man natürlich sagen, dass dieser „Mafiaboy" kriminell war; aber die von „Mafiaboy" benutzten Mittel waren nur einsetzbar, weil diese Technik so schwach ist, dass sie nicht mal mehr ein Vorhängeschloss hat, mit dem man eine Haustür abschließen kann.

Meine Damen und Herren, es kommt leider noch schlimmer. Denn das Internet, wie wir es heute benutzen, ist für Geschäftskommunikation deshalb ungeeignet, weil es auf 13 zentralen Verwaltungsservern, den so genannten Root-Servern, basiert. Wenn diese angegriffen werden, kann das Internet total lahmgelegt werden. Ein Probeangriff dieser Art ist im Oktober 2002 passiert, hat eine Stunde gedauert und hat von den 13 Servern sechs zum Absturz gebracht. Die Architektur, die wir hier haben, ist folgende: In der Mitte steht ein großer Server (A genannt), darunter sind weitere zwölf Server in USA, Europa und Japan. Und davon hängen alle anderen (z. B. der deutsche Server „denic") ab. Die Internetadressierung erfolgt bekanntlich über vier Paare von Zahlen zwischen einer und drei Ziffern; die müssen übersetzt werden in zum Beispiel: bka.org. oder bka.de – also in eine logische Adresse. Das macht der Domänendienst (domain name service: DNS). Werden diese DNS-Dienste blockiert, kann das Internet lahm gelegt werden.

Meine Damen und Herren, was machen wir heute, um uns gegen die vielfältigen Gefahren zu schützen? Wir stellen unsere Informationstechnik im Unternehmen in einen „Turm“ (Tower of IT), so wie die Queen ihre Kronjuwelen dadurch schützt, dass sie außen eine dicke Mauer mit Wällen, darauf Stacheldraht, innen Hunde und Wachleute mit Maschinenpistolen und viele Gänge hat. Ganz tief innen drinnen im Turm sind die Kronjuwelen, und die stiehlt keiner, weil es so viele Schutzmechanismen gibt, sie zu schützen. So ähnlich macht man das auch mit Computern und Netzen: man legt um die Netze und Computer immer mehr Ringe von Schutzmechanismen, die heißen Antiviren, Einbruchsentdeckende Systeme (intrusion detection systems); Nachrichten werden verschlüsselt, Feuerwälle (firewalls) sollen gegen Hacker schützen. Was man damit macht, ist aber widersinnig. Wenn man nämlich die Sicherheit deshalb nicht gewährleisten kann, weil die Systeme schon viel zu komplex sind, dann kann es keine Lösung sein, die schon komplexen Systeme mit weiterer Komplexität zu umgeben und sie dadurch sicherer zu machen. Dieses heißt nämlich, den Teufel mit dem Beelzebub auszutreiben. Und das ist widersinnig, auch wenn wir es heute so versuchen.

Anforderungen an beherrschbare Informationstechniken

Es gibt nur einen Weg zur Verringerung der Risiken und zur Erhöhung der Sicherheit: die Spezifikationen müssen geändert werden. Statt auf Personal Computing müssen wir auf Safe Computing setzen. Ein Beispiel, wenn Ihr System abstürzt: „Wieso stürzt das ganze System ab, bloß weil irgendein Programm falsch oder ein Systemteil falsch programmiert ist?“ Bei den frühen Großrechnern kannte man das Prinzip des „Benign Degradation“. Das System schützt die Nachbarteile eines abstürzenden Systemteils, sodass Dokumente, die wir gerade erstellen, nicht gleichzeitig mit abstürzen und verloren gehen. Ein weiteres Beispiel: wenn wir Vertrauen in E-Commerce aufbauen wollen, dann muss auch garantiert werden, dass meine Bank einen Dienst nicht einfach ablehnen kann (Nichtzurückweisbarkeit). Und der Händler muss darauf vertrauen, dass wir nicht sagen: „Das habe ich aber gar nicht angefordert“ (Nichtabstreitbarkeit).

Die Zukunft sicherer Systeme, wie ich sie mir vorstelle, sieht so aus: Es gibt viele Applikationen, wo wir auch mit unsicheren Systemen arbeiten können. Wenn man im Internet surft und irgendein schönes Video oder was auch immer angucken wollen: Warum braucht man Sicherheit? Aber wenn man der Firma oder Behörde wichtige und vertrauliche Nachrichten versenden will, dann muss man sich darauf verlassen, dass die Kommunikation in Ordnung ist, nicht gefälscht und angegriffen werden kann.

Das heißt, wir werden Bereiche haben, in denen können wir auf Sicherheit verzichten können. Man kann dann das freie, unsichere Internet benutzen. Aber in anderen Bereichen muss es *unmöglich* sein anzugreifen. Ich gehe davon aus, dass wir eines Tages solche sicheren Systeme haben.

Wie lange mag dies dauern? Wenn wir in der Größenordnung von 70–75 Jahren, in der Industriegesellschaft bis zum Dampfkesselüberwachungsverein und bei der Autoproduktion bis zum Verbraucherschutz nach Ralf Naders „Unsafe at any Speed" gebraucht haben, so könnte die analoge Entwicklung ebenfalls etwa 70 bis 75 Jahre dauern. Und jetzt addieren Sie diesen Wert zum Startjahr 1941, dann kommen Sie auf etwa 2020–2025. Das heißt: bis dahin werden die Unfälle zunehmen, und die immer stärkeren Schäden werden den Verbraucherschutz und sichere Systeme erst erzwingen. Dann wird auch Microsoft die Schäden, die durch Versagen ihrer Software entstehen, ersetzen müssen, wie heute die Hersteller von Autos. Erst dann wird die Informationsgesellschaft zu einer Gesellschaft, in der wir virtuelle Organisationen, virtuelle Güter wirklich nur nutzen können.

Bis dahin werden allerdings die Unfälle zunehmen. Und deshalb sage ich meinen Studenten, denen ich Sicherheitstechniken und Risikoanalyse beibringe: „Ihr werdet noch einen viel interessanteren Job haben. Euer Job ist sicher." Und das BKA wird zunehmend Computer-kriminelle Angriffe aufzuklären haben. Viel Erfolg. Herzlichen Dank für Ihre Aufmerksamkeit!

Freiheit braucht Sicherheit – Sicherheit braucht Freiheit

Waldemar Kindler

1 Einleitung

Ich freue mich, dass ich als Leiter der Abteilung Öffentliche Sicherheit und Ordnung im Bayerischen Staatsministerium des Innern heute Gelegenheit habe, zum Thema **„Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnologien; Freiheit braucht Sicherheit – Sicherheit braucht Freiheit“** zu Ihnen zu sprechen.

Wir alle bewegen uns ständig im Spannungsfeld zwischen dem Freiheitsanspruch des Bürgers auf der einen und seinem Sicherheitsbedürfnis auf der anderen Seite. Entsprechend meiner Aufgabe möchte ich natürlich vor allem die Sicherheitsinteressen des Bürgers auf diesem Feld und damit die Interessen einer wirksamen Kriminalitätsbekämpfung vertreten. Bei der Frage, was notwendig ist, um die Sicherheit der Bevölkerung auch in Zukunft zu gewährleisten, geht es nicht darum, den polizeilichen Zuständigkeitsbereich zu erweitern – wie Herr Dr. Dix in seinem Aufsatz in der Computerwoche vom Januar 2001 schreibt. Ich bin aber der Auffassung, dass es auch bei den neuen kriminellen Erscheinungsformen im Zusammenhang mit der Informations- und Kommunikationstechnologie, keine rechtsfreien Räume für Straftäter geben darf. Aus meiner Sicht geht es vielmehr darum, – unter Abwägung der berechtigten Freiheitsbedürfnissen der Bürger – konsequent gegen diese neuartigen Kriminalitätsformen vorzugehen.

2 Wesentliche Kriminalitätsbereiche

Zunächst möchte ich versuchen, die Bereiche der Informations- und Kommunikationstechnologie darzustellen, die aus meiner Sicht unserer besonderen Aufmerksamkeit bedürfen:

Dies sind

- die Kriminalität im Internet,
- die Computerkriminalität im engeren Sinne und
- die Technologie IuK als Tatmittel.

Bei der Kriminalität im Internet sind es heute insbesondere

- die zunehmende verbotene Verbreitung pornografischer und gewaltverherrlichender Medien und
- das internationale Spektrum des Linksextremismus, Rechtsextremismus oder Ausländerextremismus,

mit dem wir uns beschäftigen müssen.

Aber auch Phänomene wie

– Kannibalismus im Internet oder
– Suizidforen

sind völlig neuartige kriminelle Erscheinungsformen, die entsprechende polizeiliche Maßnahmen erfordern.

Im Bereich der Computerkriminalität im engeren Sinne haben wir es

– mit Attacken gegen Server,
– mit in wenigen Minuten weltweit verbreiteten Viren oder Würmern,
– mit Trojanern (Trojanische Pferde sind Programme, die neben scheinbar nützlichen auch „schädliche" Programme enthalten),
– mit Wirtschaftsspionage oder
– mit der noch schwer einzuschätzenden Gefahr des so genannten Cyberterrorismus, also mit gezielten Angriffen von Terroristen auf Computernetze (z. B. von Stromversorgungsunternehmen) mit möglichen katastrophalen Folgen,

zu tun.

Hinzu kommt, dass die modernen Informations- und Kommunikationsmittel für die Planung, Vorbereitung und Koordination praktisch aller denkbaren Straftaten genutzt werden.

Für den Bereich Informationstechnik ist vor allem das Internet zu nennen. Über das werden heute zunehmend

– Kreditkarten- und Auktionsbetrügereien,
– Mehrwertdienste-Missbrauchshandlungen (0190er Nummern) oder
– Verstöße gegen das Urheberrechtsgesetz

begangen.

Das breite Feld der Telekommunikation, wie der Mobil- und Festnetz-Telefonie oder der E-Mail-Funktion, wächst beständig und verschmilzt immer stärker miteinander.

3 Problemfelder und Lösungsansätze

Ich will versuchen, Ihnen anhand nur eines aktuellen Fallbeispiels aufzuzeigen, welche Probleme im Zusammenhang mit der Kriminalität im Internet bestehen. Ich möchte Ihnen aber auch verdeutlichen, dass schrankenlos gewährte Freiheit auf diesem Feld die Sicherheit der Bürger erheblich beeinträchtigen würde.

3.1 Fallbeispiel „Pädophile Tätergruppe in München"

Das Polizeipräsidium München ermittelte seit Ende 2002 aufgrund einer Annonce in einem regionalen Anzeigenblatt und eines vertraulichen Hinweises – zu-

nächst verdeckt – gegen eine 16-köpfige pädophile Tätergruppe aus dem Großraum München. Die Gruppe trat nach außen hin als „Pädo-Selbsthilfe- und Emanzipationsgruppe München“ auf. Tatsächlich waren die Treffen jedoch Kontaktbörsen für Gleichgesinnte, bei denen die Teilnehmer Informationen über ihre pädophilen Neigungen und über Verhaltenshinweise und Schutzmaßnahmen im Umgang mit Strafverfolgungsorganen ausgetauscht haben. Die Mitglieder der Pädophilen-Gruppe – die meisten einschlägig vorbelastet – gingen dabei konspirativ und arbeitsteilig vor. Wir ermitteln deshalb gegen den Pädophilen-Ring wegen des Verdachts

– der Bildung einer kriminellen Vereinigung,
– des sexuellen Missbrauchs von Kindern sowie
– des Besitzes und der Verbreitung kinderpornografischen Materials.

Am 30. Oktober wurden insgesamt 18 Objekte in fünf Städten und Gemeinden durchsucht. Gegen zwölf der 16 angetroffenen Beschuldigten erging Untersuchungs-Haftbefehl. Derzeit befinden sich acht Personen in Haft.

3.2 Auswertung sichergestellter Datenträger

Im Rahmen der Durchsuchungen konnte umfangreiches Beweismaterial sichergestellt werden. Es handelt sich unter anderem um 42 Computer beziehungsweise Laptops, 48 externe Festplatten, 3.942 CD-ROM, 4.200 Disketten, 1.184 Videokassetten und mehrere tausend Dias. Das Datenvolumen eines der sichergestellten PCs hätte ausgereicht, um damit zum Beispiel alle Videos einer mittleren Erwachsenenvideothek abspeichern zu können.

Sie können sich sicher vorstellen, dass die beweiskräftige Auswertung der sichergestellten Datenträger die Ermittlungsbehörden vor riesige Herausforderungen stellt.

Wir beauftragen deshalb in Abstimmung mit der Staatsanwaltschaft vermehrt externe Gutachter mit der Auswertung sichergestellter PC-Anlagen und Datenträger. Um sichergestellte Videos beweiskräftig auswerten zu können, ob beziehungsweise welche inkriminierte Inhalte darauf vorhanden sind, haben wir inzwischen mit Hilfe einer privaten Firma eine spezielle Software entwickelt. Damit sind wir in der Lage, Filme anhand von Bilderübersichten am PC in kurzer Zeit zuverlässig und gerichtsverwertbar auszuwerten. Ein bislang noch ungelöstes Problem in diesem Zusammenhang stellt die Analyse von Filmen und Bilddaten hinsichtlich der Zusammenführung der abgebildeten Opfer, Täter oder der Tatörtlichkeiten dar. Hier stehen derzeit keine ausreichenden technischen Hilfsmittel zur Verfügung.

Das Spannungsfeld zwischen Freiheit und Sicherheit beleuchteten Waldemar Kindler aus der Sicht der Polizei . . . . . .

3.3 Freiheit im Netz vs. Sicherheitsinteressen der Bürger

Diese neuen Erscheinungsformen der Kriminalität im Internet stellen die Polizei vor riesige Probleme. Während früher in Pädophilenkreisen Bücher und Hefte „unter dem Ladentisch" verkauft wurden, bietet das „World-Wide-Web" völlig neue Verbreitungswege für die Kriminellen. Grenzenlose Freiheit im Netz würde bedeuten, dass beispielsweise „Kinderschänder" ihre perversen Neigungen ungehindert und ungestraft ausleben könnten und unzählige, unschuldige Kinder zu Opfern würden. Kein vernünftiger Mensch kann die „Freiheit im Netz" als oberste Prämisse ansehen, sondern der Gesetzgeber muss hier entsprechende Regelungen schaffen, die einen Missbrauch der neuen Medien verhindert. Neben der Polizei sind alle gesellschaftlichen Gruppen aufgefordert, diesen Kriminellen Einhalt zu gebieten.

Ich möchte hier nochmals betonen, dass eine lückenlose Überwachung des WEB (= Internet) weder gewünscht noch tatsächlich möglich ist.

3.4 Zunehmender Einsatz der Kryptografie

Ein spezielles Problemfeld ergibt sich im Spannungsfeld von berechtigtem Anspruch des Bürgers auf Freiheit und Sicherheit beispielsweise im Geschäftsverkehr und dem Sicherheitsanspruch des Staates durch den zunehmenden Einsatz der Kryptografie.

Die Kryptografie ist grundsätzlich für

- den Datenschutz des rechtschaffenen Bürgers,
- die Entwicklung des elektronischen Geschäftsverkehrs und
- den Schutz von Unternehmensgeheimnissen

sicher notwendig und sinnvoll, aber im Ermittlungsfall für die Erfüllung des polizeilichen Auftrags ein weiteres bedeutendes Hindernis. Denn auch die Kriminellen setzen zunehmend Verschlüsselungstechniken für ihre Zwecke ein. Die überall frei erhältlichen Verschlüsselungstechniken werden dabei sowohl für die Datenübertragung als auch für die Sicherung von Daten auf Datenträgern eingesetzt. Dies bedeutet, dass die Polizei auf kriminelle Daten keinen Zugriff mehr hat.

Mitglieder des Münchner Pädophilen-Rings haben die Verschlüsselungstechniken auch zur Absicherung ihrer gespeicherten Daten verwendet. Dadurch haben wir zwei Problemstellungen:

1. Einmal können wir bei der Auswertung der Datenträger nicht alle inkriminierten Inhalte erkennen, weil sie zum Beispiel mit Hilfe der Steganografie (Steganografie = ein spezielles Verfahren zur Verschlüsselung von Daten. Bei der Steganografie werden geheime Daten unsichtbar in eine Trägerdatei eingebettet.) gut versteckt wurden.
2. Zum Zweiten können wir zwar auf den Datenträgern erkennen, dass hier Daten verschlüsselt vorhanden sind, können sie aber ohne den entsprechenden „Schlüssel“ nicht lesen.

Ich darf hierzu anmerken, dass für mich der Gedanke, umfangreiche kinderpornografische Dateien unter Umständen an die Täter zurückgeben zu müssen, weil wir ihre strafbaren Inhalte aufgrund der Verschlüsselung nicht nachweisen können, unerträglich ist.

Um vor solchen Entwicklungen nicht kapitulieren zu müssen, halten ich es für dringend erforderlich, dass wir gemeinsam unsere Bemühungen um Problemlösungen weiter verstärken. Zum Beispiel sollten wir erneut darüber nachdenken, ob nicht ein „Trust-Center“ (Trust-Center = Vertrauenszentrum, das die Identität einer Person bestätigt. In dem TC werden die „Schlüssel“ verwaltet.) geschaffen werden muss, das mit Hilfe der Hersteller der Verschlüsselungstechniken in der Lage ist, im Einzelfall und auf richterliche Anordnung verschlüsselte Dateien zu entschlüsseln.

3.5 Speicherung von Verbindungsdaten

Ein weiteres drängendes Problem im Spannungsfeld zwischen der Freiheit im Netz und dem Strafverfolgungsanspruch des Staates ist die fehlende Pflicht für Provider und Servicebetreiber zur Speicherung von Verbindungsdaten, die wir

zur Identifizierung von Straftätern brauchen. Diese Daten werden entsprechend der aktuellen Rechtslage oft bereits kurze Zeit nach Beendigung der Datenübertragung gelöscht oder in vielen Fällen überhaupt nicht aufgezeichnet.

Obwohl im Falle des Münchner Pädophilen-Rings die Auswertung der umfangreichen Datenträger mit Nachdruck betrieben wird, müssen wir derzeit mit einer Auswertedauer von drei bis vier Monaten rechnen. Nachdem jedoch die Verbindungsdaten von den Providern und Servicebetreibern entweder gar nicht gespeichert oder bereits nach kurzer Zeit wieder gelöscht werden, können in vielen Fällen wichtige Kommunikationsverbindungen nicht mehr nachvollzogen und für die Ermittlungen genutzt werden. Aus diesem Grund halten ich es für eine effektive Verfolgung von Kinderschändern, Terroristen oder Betrügern für notwendig, eine bis zu zwölfmonatige Mindestspeicherfrist für Telekommunikationsverbindungsdaten gesetzlich zu normieren.

Den Diensteanbietern soll dabei eine befristete Sicherung der ohnehin zu Abrechnungszwecken gewonnenen Verbindungsdaten aufgegeben werden. Eine solchermaßen befristete Speicherung ist unter dem Blickwinkel der Bedürfnisse einer effektiven Strafverfolgung und wirksamen Gefahrenabwehr durchaus zumutbar.

In der Abwägung zwischen effektiver Verbrechensbekämpfung einerseits und datenschutzrechtlichen Belangen sowie finanziellen Interessen der Telekommunikationsunternehmen anderseits erscheint uns eine solche Frist auch angemessen.

Nicht nur die Innenministerkonferenz und der Bundesrat haben in den letzten Jahren wiederholt entsprechende Beschlüsse gefasst, um Verbesserungen für die Strafverfolgungsbehörden zu erreichen. Auch auf EU-Ebene hat es unter dänischer Präsidentschaft im vergangenen Jahr eine solche Initiative gegeben.

Der Bundesgesetzgeber ist aufgefordert, diese Speicherverpflichtung für die Diensteanbieter schnellstmöglich gesetzlich umzusetzen, damit wir gegen Kinderschänder und andere Kriminelle nachhaltig vorgehen können. Denn vergessen wir nicht: Hinter jedem kinderpornografischen Bild steht ein schwer missbrauchtes Kind, das unsagbare Qualen erlitten hat. Als Sicherheitsbehörden haben wir die Pflicht, jedes potentielle Opfer bestmöglich zu schützen.

3.6 Cyber-Crime-Übereinkommen

Darüber hinaus haben die Fälle der letzten Jahre aber auch gezeigt, dass der Kampf gegen Kinderpornografie und andere Formen der sexuellen Ausbeutung von Kindern und Jugendlichen, aber auch gegen die verschiedenen Formen der Computerkriminalität aufgrund der Internationalität der Datennetze nicht mehr nur national geführt werden kann, sondern eine internationale Bekämpfung dieser Kriminalitätsphänomene unabdingbar ist.

Ich bedaure es deshalb sehr, dass es in den Strafgesetzbüchern der europäischen Staaten immer noch keine einheitliche Definition gibt, bis zu welchem Lebensalter ein Opfer als Kind zu werten ist. Auch ist der Besitz von Kinderpornografie noch nicht in allen Staaten strafbar.

Ähnlich ist es im Kriminalitätsfeld des Extremismus, da beispielsweise rechtsextremistische Propaganda in den meisten ausländischen Staaten nicht strafbewehrt ist.

Beispielhaft nennen will ich hier nur die Verbreitung der „Auschwitz-Lüge". Die Einstellung von derartigen Inhalten ist beispielsweise in den USA nicht strafbar.

Andererseits ist die Strafverfolgung im Inland nach der Rechtsprechung des Bundesgerichtshofs bei Volksverhetzung in Gestalt der Auschwitz-Lüge auch dann möglich, wenn die fraglichen Äußerungen auf einem ausländischen Server in das Internet eingestellt werden, der Internetnutzern in Deutschland zugänglich ist.

Ein wichtiger Schritt, hier Verbesserungen zu erreichen, ist die Cyber-Crime-Convention des Europarats, die am 23. November 2001 in Budapest unterzeichnet wurde.

Wir versprechen uns vom Cyber-Crime-Übereinkommen insbesondere

- Erleichterungen bei der Ermittlung und Verfolgung einschlägiger Straftaten,
- eine Anpassung des Computerstrafrechts,
- internationale Schutzstandards bei der Kinderpornografie und
- die Erleichterung und Beschleunigung der internationalen Zusammenarbeit über eine möglichst umfassende Rechtshilfe.

Auch hier ist der Gesetzgeber gefordert, die Maßnahmen des Übereinkommens in nationales Recht umzusetzen. Auch hier besteht dringender Handlungsbedarf.

3.7 Anlassunabhängige Fahndung im Internet

Nun aber zu einem weiteren Thema, der anlass-unabhängigen Fahndung im Internet. Die Freiheit im Netz muss immer dann seine Grenzen haben, wenn Straftaten begangen wurden. Nach einer Forsa-Umfrage vom Juni 2003 nutzen etwa 33,8 Millionen Menschen, also fast 53 % der Bevölkerung in Deutschland, das Internet. Im Internet werden pro Tag Zehntausende neuer Seiten eingestellt. Wie viele Seiten es gibt, weiß man nicht genau. Die bekannteste Suchmaschine „Google" zum Beispiel durchstöbert insgesamt mehr als drei Milliarden Webseiten. Hinzu kommen File-Sharing-Systeme, Tausende von Newsgroups und Internet-Chat-Räume. Damit einhergehend nimmt die verbotene Verbreitung pornografischer und gewaltverherrlichender Schriften beständig zu. Linksextremisten, Rechtsextremisten und Ausländerextremisten nutzen das Internet intensiv als internationale Plattform zur Verbreitung ihrer gefährlichen Ideologien und zum gezielten

Informationsaustausch untereinander. Immer wieder neue Phänomene, wie Kannibalismus oder Suizidforen, erfordern polizeiliches Tätigwerden.

In Anbetracht dieser Entwicklungen sehe ich die Gefahr, dass im Internet vermehrt rechtsfreie Räume entstehen könnten. Bei allen Schwierigkeiten, die mit dem globalen Internet verbunden sind, dürfen wir solche Entwicklungen nicht zulassen.

Ich weiß, dass viele Eltern zu Hause keinen Internetzugang einrichten, weil sie Angst haben, ihre Kinder könnten

- mit jugendgefährdenden Inhalten wie Porno-, Hass- oder grausamsten Gewaltdarstellungen konfrontiert werden,
- über Chat-Foren in Suizidkreise geraten oder
- mit gefährlichem extremistischem Gedankengut mit unabsehbaren Folgen in Berührung kommen.

Solche Zustände sind für mich eine gravierende Beeinträchtigung der Freiheit – nicht aber die notwendigen Eingriffsmaßnahmen der Polizei gegenüber erkannten Straftätern. Wir brauchen eine angemessene Sozialkontrolle im Netz – auch durch die Polizei. Ich plädiere dafür, die anlassunabhängige Fahndung im Internet durch die Polizei, wie sie beim Bayerischen Landeskriminalamt und im Bundeskriminalamt bereits praktiziert wird, auch in anderen Bundesländern institutionalisiert durchzuführen.

3.8 Wirtschaft

Sehr geehrte Damen und Herren, eine wichtige Funktion zum Schutz vor kriminellen Machenschaften im Internet kommt hierbei insbesondere auch den Providern zu. Sie sind ein Stück weit auch dafür verantwortlich, dass die im Netz angebotenen Inhalte nicht gegen Strafgesetze verstoßen. Im Gegensatz zur staatlichen Gesetzgebung besitzen die international tätigen Online-Dienste, Internet-Provider und E-Commerce-Unternehmen die nötige Flexibilität, um über nationale und internationale Vereinbarungen staatlichen Rechtsvereinheitlichungen voranzugehen. Dies gilt nicht nur für jugendgefährdende Inhalte, sondern auch für die Unterstützung der Strafverfolgungsbehörden. Sie müssen aus meiner Sicht ihrer Verantwortung für ein sicheres Internet noch stärker gerecht werden und die vorhandenen Möglichkeiten dazu nutzen.

Ganz generell müssen wir heute von der Wirtschaft erwarten können, dass sie sich

- zum einen mit den sich ständig weiter verändernden Risiken und Problemen bei der Nutzung der modernen Informations- und Kommunikationstechnologie noch stärker auseinandersetzt und sich
- zum anderen an der Entwicklung und Umsetzung verbindlicher präventiver Strategien noch stärker aktiv und innovativ beteiligt.

3.9 Nutzer der IuK

Aber auch vom Nutzer der modernen IuK müssen wir heute sowohl im privaten wie im Geschäftsbereich zunehmend einfordern, dass er

- sich mit den Möglichkeiten, Bedingungen und Gefahren dieser Kommunikation auseinandersetzt,
- die für einen sachgerechten Umgang erforderlichen Kompetenzen sukzessive auf- und ausbaut und
- eigene Präventionsanstrengungen unternimmt.

Eine Ausnahme ist hier sicher bei Kindern und Jugendlichen sowie bei Nutzern im Seniorenalter zu machen, bei denen die dazu notwendigen Kenntnisse noch nicht oder nicht mehr hinreichend erwartet werden können. Für diese Gruppen müssen die technischen Schutzmöglichkeiten, wie zum Beispiel Filtersysteme zum Schutz vor jugendgefährdenden Inhalten, weiter verbessert und die Medienkompetenz durch einfache, verständliche und zielgruppengerechte Informationen weiter optimiert werden.

3.10 Speicherung der Kundendaten von Prepaid-Karten-Inhabern

Abschließend will ich noch zwei weitere Problembereiche der Kriminalität im Zusammenhang mit der IuK unter dem Gesichtspunkt Datenschutz und Polizei beleuchten:

Dies sind

- Nutzung von Pre-Paid-Handys und
- präventive Telekommunikationsüberwachung.

Die weit verbreitete Nutzung von Prepaid-Handys stellen für die Ermittlungsbehörden ein generelles Problem dar.

Mehr als 70 % der Bevölkerung besitzt mittlerweile ein Handy. Etwa 60 % dieser über 59 Millionen Mobilfunkteilnehmer benutzen Prepaid-Karten. Vor allem im Bereich der Organisierten Kriminalität, im Rauschgifthandel und im Bereich der Staatsschutzkriminalität werden solche Prepaid-Karten intensiv genutzt, um möglichst unentdeckt agieren zu können. Weil wir bisher nur teilweise erheben können, an wen solche Prepaid-Karten ausgegeben wurden, haben wir bei der Überwachung der Telekommunikation erhebliche Schwierigkeiten. Oft können wir nur zum Teil und mit Hilfe des Einsatzes von IMSI-Catchern mit unverhältnismäßig hohem technischen und personellen Aufwand feststellen, welches Handy von wem benutzt wird.

Das Bundesverwaltungsgericht hat am 22. Oktober entschieden, dass die Anbieter von Prepaid-Karten nach derzeitiger Rechtslage nicht verpflichtet sind, entsprechende Daten ihrer Kunden zu erheben, zu überprüfen und in eine Kunden-

datei einzustellen. Die Strafverfolgungsbehörden müssen jedoch auch künftig in der Lage sein, mit Hilfe der Überwachung der Telekommunikation kriminelle Organisationen aufzuklären und zu zerschlagen. Daher muss der Bundesgesetzgeber schnellstmöglich für eine klare und praxisgerechte Regelung zur Speicherung und Erhebung personenbezogener Daten durch die Anbieter von Prepaid-Telefonkarten sorgen.

3.11 Präventive Telekommunikationsüberwachung

Die Polizei muss aber auch in der Lage sein, die neuen Informations- und Kommunikationstechnologien primär zur Gefahrenabwehr nutzen können. Hier stoßen wir derzeit jedoch vielfach an rechtliche Grenzen, da die meisten Befugnisse an Strafverfolgungszwecke geknüpft sind. Beispielsweise haben wir in Fällen, in denen Personen in Suizid-Foren im Internet aktuell ihren Freitod ankündigen, keine Befugnis, um von den Providern die notwendigen Verbindungsdaten anzufordern. In anderen Fällen müssen wir abwarten, bis die entsprechenden Tatbestände hinreichend konkret belegt sind, bevor wir die Kommunikation potenzieller Gefährder überwachen dürfen. Wir müssen praktisch abwarten, bis die Tat begangen ist, bevor wir handeln können.

Hier muss das Recht den fachlichen Anforderungen – immer unter Abwägung der Freiheitsrechte des Bürgers einerseits und den Sicherheitsinteressen andererseits – angepasst werden. Bayern plant daher, die präventive Telekommunikationsüberwachung im Bayer. Polizeiaufgabengesetz zu normieren. Inwieweit hier Berufsgeheimnisträger und Journalisten ausgenommen werden können und sollen, werden wir überlegen und sorgsam abwägen.

4 Schlussbemerkung

Mit den Gefahren und Herausforderungen, die die fortschreitenden Entwicklungen in der Informations- und Kommunikationstechnik mit sich bringen, müssen wir uns in allen Bereichen unserer Gesellschaft auch künftig intensiv auseinandersetzen. Ich weiß, dass ich hier mit dem einen oder anderen Datenschutzbeauftragten nicht in allen Punkten übereinstimme.

Dies gilt insbesondere

- in Fragen der Kryptografie,
- bei der Verpflichtung von Providern und Servicebetreibern zur Speicherung von Telekommunikationsverbindungsdaten,
- bei der Speicherung von Prepaid-Karten-Inhabern oder
- in Fragen der Telekommunikationsüberwachung.

Lassen Sie mich daher noch einmal betonen: Es geht uns nicht darum, den gläsernen Bürger zu schaffen oder einen Überwachungsstaat einzuführen. Gerade für

mich als Juristen und obersten Polizeichef der Bayerischen Polizei ist die Freiheit ein hohes Gut.

Aber:

Wir wollen die Freiheit des Bürgers auch dadurch erhalten, indem wir seine Sicherheit bestmöglich gewährleisten. Wir wollen Kinderschändern und Terroristen das Handwerk legen und Personen, die in Gefahr sind, schnell und zuverlässig helfen können. Dazu brauchen wir die notwendigen gesetzlichen Grundlagen. In diesem Sinne appelliere ich an jeden Einzelnen, der für die Sicherheit in unserem Lande Verantwortung trägt: Achten wir gemeinsam darauf, dass einerseits die Freiheit der Bürger und der sichere Geschäftsverkehr weitgehend erhalten bleiben, andererseits dürfen wir nicht aus falsch verstandenen Liberalisierungsbemühungen Entwicklungen zulassen, die in gefährlichen rechtsfreien Räumen münden oder zu nicht hinnehmbaren Beeinträchtigungen der Sicherheit der Bevölkerung führen.

Freiheit braucht Sicherheit – Sicherheit braucht Freiheit

Alexander Dix

Benjamin Franklin und die Freiheit zur unbeobachteten Kommunikation

Zwölf Thesen

Die Balance zwischen Freiheit und Sicherheit ist in letzter Zeit – gerade nach den Anschlägen vom 11. September – wiederholt sehr grundsätzlich diskutiert worden. In diesem Zusammenhang ist auch ein Satz von Benjamin Franklin, einem der Gründerväter der Vereinigten Staaten von Amerika, – allerdings meist unrichtig – zitiert worden, der da lautet: „Diejenigen, die bereit sind, eine wesentliche Freiheit aufzugeben, um ein wenig vorübergehende Sicherheit zu erlangen, verdienen weder Freiheit noch Sicherheit."[1]

Auch wenn der moralische Unterton in diesem Satz irritieren mag, erscheint es lohnend, sich mit diesem Ausspruch vor dem Hintergrund der modernen Informations- und Kommunikationstechnik auseinander zu setzen.

1. Das Telekommunikationsgeheimnis ist das zentrale Menschenrecht (die „wesentliche Freiheit" im Franklinschen Sinne) in der Informationsgesellschaft. Das Bundesverfassungsgericht betont in ständiger Rechtsprechung, dass die Nutzung von Kommunikationsmedien „in allem" (also sowohl hinsichtlich des Inhalts als auch hinsichtlich der Umstände) vertraulich möglich sein soll.[2] Auf diese Weise sollen die Bedingungen einer freien Telekommunikation überhaupt aufrecht erhalten werden. Dieser Schutz muss sich nach meiner Überzeugung auch auf die Nutzung von Tele- und Mediendiensten (insbesondere also des WorldWideWeb) erstrecken, die auf der Grundlage der Telekommunikation erbracht werden.

2. Wie das Grundrecht auf Datenschutz schützt auch das Telekommunikationsgeheimnis nicht lediglich ein Individualinteresse, sondern zugleich das Gemeinwohl. Jede heimliche Überwachung des Fernmeldeverkehrs betrifft die Kommunikation der Gesellschaft insgesamt und gefährdet ihre Qualität. Wörtlich hat das Bundesverfassungsgericht im so genannten Journalisten-Urteil vom März 2003 formuliert: *„Es gefährdet die Unbefangenheit der Telekommunikation und in der Folge die Qualität der Kommunikation einer Gesellschaft, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen."*[3] Diese Feststellung hat auch angesichts der Bedrohung durch den inter-

1 „They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Historical Review of Pennsylvania (1759).

2 BVerfGE 100, 313, 358 (Verdachtslose Rasterfahndung durch den BND).

3 BVerfG, Urteil v. 12. 3. 2003, NJW 2003, 1787, 1793.

..... und Dr. Alexander Dix aus der Sicht des Datenschutzes

nationalen Terrorismus oder neue Formen der Computerkriminalität und in Anbetracht der offenbar zunehmenden Verbreitung kinderpornographischer Bilder oder rassistischer Hetze („hate speech") im Internet nichts von ihrer Berechtigung verloren.[4]

Herr Schily hat in seiner Eröffnungsrede von der Bedeutung des subjektiven Sicherheitsgefühls gesprochen. Wenn man diese Kategorie verwendet (und das erscheint durchaus legitim), dann sollte auch das vom Verfassungsgericht beschriebene Gefühl des Überwachtwerdens in die Gesamtbetrachtung miteinbezogen werden, das durch breit gestreute staatliche Überwachungsmaßnahmen zu entstehen droht, die in der guten Absicht ergriffen werden, um ein subjektives Sicherheitsgefühl zu erzeugen oder wiederherzustellen.

4 Vgl. Hoffmann-Riem in: Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht (Hrsg.), Internationales Symposium „Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union", Potsdamer Materialien zu Akteneinsicht und Informationszugang Bd. 2, 2001, 23, 41 ff.; Limbach, Recht der Datenverarbeitung 2002, 163, 165.

3. Die Freiheit der vertraulichen Telekommunikation gilt allerdings nicht uneingeschränkt. Einschränkungen sind zulässig, wenn sie dem legitimen öffentlichen Zweck der Aufklärung und Verfolgung schwerer Straftaten dienen, wobei die Liste dieser schweren Straftaten ständig wächst und bisher noch keiner kritischen Überprüfung unterzogen worden ist. Der Eindruck drängt sich auf, dass nahezu bei jeder neuen Kriminalitätsform, die gesellschaftlich als besonders verwerflich gilt, sehr schnell nach Einschränkungen des Telekommunikationsgeheimnisses gerufen wird. Jüngste Beispiele sind die Korruption und die Schwarzarbeit. Einschränkungen des Telekommunikationsgeheimnisses sind aber nicht schon dann verfassungskonform, wenn sie allgemein Zwecken der zukünftigen Strafverfolgung dienen. Vielmehr muss – so dass Bundesverfassungsgericht in der zitierten Journalisten-Entscheidung – ein konkreter Tatverdacht für eine Straftat von erheblicher Bedeutung vorliegen und es müssen hinreichend sichere Tatsachen für die Annahme sprechen, dass die überwachte Person, wenn sie nicht mit dem Beschuldigten identisch ist, für ihn als Nachrichtenmittler auftritt.[5]

4. Aus dieser Aussage des Bundesverfassungsgerichts kann nur der Schluss gezogen werden, dass eine anlassunabhängige, verdachtslose Überwachung des Telekommunikations- und Internetverkehrs auf Vorrat (sog. Verdachtsgewinnungseingriff) mit dem Grundgesetz nicht zu vereinbaren ist. Bezüglich der Überwachung und Aufzeichnung von Gesprächsinhalten dürfte das – bisher zumindest – unbestritten sein. Es gilt aber in gleicher Weise für den jüngsten Vorschlag des Rechtsausschusses des Bundesrates zum Entwurf des Telekommunikationsgesetzes, nach dem Provider zur Speicherung aller Verkehrsdaten[6] für ein halbes Jahr verpflichtet werden sollen.[7] Bereits die Speicherung (nicht erst die Verwendung) der Daten zu den näheren Umständen aller stattfindenden Kommunikationsverbindungen (wer hat wann wie lange von wo aus mit wem kommuniziert?) über den für die Rechnungslegung erforderlichen Zeitraum hinaus ist ein unverhältnismäßiger Eingriff in das Telekommunikationsgeheimnis. Das Bundesverfassungsgericht unterscheidet zwar zwischen der Überwachung von Gesprächsinhalten und der Überwachung der Kommunikationsumstände, es sieht aber auch in letzterer einen schwerwiegenden Grundrechtseingriff.[8] Wer moderne Kommunikationsnetze nutzt, darf nicht

5 So das BVerfG, NJW 2003, 1791.

6 Die Novelle zum Telekommunikationsgesetz verwendet entsprechend der EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation den neuen Begriff der Verkehrsdaten, der die im geltenden deutschen Recht verwendeten Begriffe der Verbindungs- und Abrechnungsdaten zusammenfasst. Das EU-Recht zählt auch die Nutzungsdaten, die bei der Nutzung von Tele- und Mediendiensten entstehen, zu den Verkehrsdaten. Die Erhebung und Verarbeitung von Nutzungsdaten ist in Deutschland allerdings außerhalb des Telekommunikationsgesetzes im Teledienstedatenschutzgesetz und im Mediendienste-Staatsvertrag geregelt.

7 Dem Votum des Rechtsausschusses ist das Plenum des Bundesrates am 19. 12. 2003 in seiner Stellungnahme zum TKG-Entwurf der Bundesregierung trotz der entgegenstehenden Auffassung des Wirtschaftsausschusses mehrheitlich gefolgt (BR-Drs.755/03–Beschluss).

8 BVerfG a. a. O., S. 1790.

zum bloßen Objekt einer Datenverarbeitung für unbestimmte staatliche Zwecke gemacht werden.

5. Eine routinemäßige, verdachtsunabhängige Speicherung sämtlicher Verkehrsdaten, um eine mögliche Strafverfolgung in der Zukunft zu erleichtern, wäre nicht nur verfassungswidrig, sondern auch unvereinbar mit der Europäischen Menschenrechtskonvention (Art. 8). Danach setzen Einschränkungen des Rechts auf Privatsphäre und des Telekommunikationsgeheimnisses ein „zwingendes gesellschaftliches Bedürfnis" voraus und müssen verhältnismäßig sein.[9] Die abstrakte Möglichkeit, dass der Zugriff auf massenhaft gespeicherte Verkehrsdaten in der Zukunft die Strafverfolgung erleichtern könnte, reicht dafür nicht aus. Nicht alles, was der Verbrechensbekämpfung und Strafverfolgung nützt, ist in einer demokratischen Gesellschaft auch notwendig und damit gerechtfertigt. Auch die vom Europäischen Gerichtshof für Menschenrechte geforderte Vorhersehbarkeit staatlicher Eingriffe wäre nicht gegeben, wenn unterschieds- und voraussetzungslos jede Nutzung von Informations- und Kommunikationsnetzen vom Staat oder in seinem Auftrag registriert würde.[10] Einzelne Nutzerinnen und Nutzer könnten nicht vorhersehen, unter welchen Voraussetzungen sie mit einer Überwachung ihrer Kommunikation rechnen müssten. Die Gewissheit, dass für staatliche Zwecke jede Form der Kommunikation registriert wird, ist nicht mit einer Vorhersehbarkeit im Sinne der Konvention gleichzusetzen. Zudem wäre eine flächendeckende Erhebung von Verkehrsdaten unabhängig von den Zwecken der Anbieter (insbesondere der Abrechnung) nicht nur nach deutschem Verfassungsrecht, sondern auch im Sinne der Menschenrechtskonvention unverhältnismäßig.

   Denkbar wäre dagegen ein anlassbezogenes Einfrieren vorhandener Verkehrsdaten im Einzelfall bis zu einer richterlichen Entscheidung über die Verwertung nach dem Prinzip „fast freeze – quick thaw", wie es auch die bisher nicht in Kraft getretene Cybercrime-Konvention des Europarates vorsieht. Dafür müsste allerdings zunächst das deutsche Strafverfahrensrecht geändert werden.
   Ich betone diese prinzipiellen Grenzen jeder Vorratsdatenspeicherung nicht allein vor dem Hintergrund der Auseinandersetzung um das ANON-Projekt der TU Dresden, sondern auch, weil die weitere Entwicklung zukünftiger datenschutzfreundlicher (datenarmer) Kommunikationsprotokolle nicht durch pauschale Identifikationspflichten vereitelt werden darf.

6. Immer mehr Lebensäußerungen finden in Telekommunikationsnetzen statt. Diese Entwicklung wird durch das Vordringen einer allgegenwärtigen Re-

9 Eingehend dazu das im Auftrag der britischen Bürgerrechtsorganisation Privacy International erstellte Gutachten (Memorandum of Laws Concerning the Legality of Data Retention with Regard to the Rights Guaranteed by the European Convention on Human Rights vom 10. 10. 2003. http:/www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf)

10 S. Memorandum ebda. (FN 8).

chentechnik („ubiquitous computing“) oder von umgebender Intelligenz („ambient intelligence“) noch verstärkt werden. Intelligenz wird in Gebrauchsgegenstände des täglichen Lebens wie zum Beispiel Kleidungsstücke integriert („wearable computing“, „wearware“). Mikrochips und Sensoren mit passiven oder aktiven Funkkapazitäten (Radio-Frequency Identification – RFID) können die Bewegungen der Menschen umfassend registrieren. Standortbezogene Dienste werden schon jetzt in den Mobilfunknetzen angeboten und mit dem *roll-out* des UMTS-Netzes noch erheblich erweitert. Verbesserte Möglichkeiten des Identitätsmanagements werden bald zur Verfügung stehen, die informationelle Selbstbestimmung technisch unterstützen werden. Das Institut für vorausschauende technologische Studien der Europäischen Kommission hat im Juli 2003 hierzu eine wegweisende Studie veröffentlicht[11], an der auch Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein mitgewirkt haben. Nicht nur die Reaktionen der Gesetzgeber auf die Terroranschläge des 11. September, sondern insbesondere diese technologische Entwicklung erfordert eine Neubestimmung der Balance zwischen Freiheit (Schutz der Privatsphäre) und Sicherheit. Dabei wird zunehmend deutlich, dass dem Schutz der Privatsphäre und dem Recht auf vertrauliche Kommunikation wieder mehr Bedeutung zukommen wird.

Exkurs: Der Bundesgesetzgeber hat im Juli 2002 den Einsatz des IMSI-Catchers durch die Aufnahme des § 100 i in die Strafprozessordnung legalisiert.[12] Dabei hat er davon abgesehen, Artikel 10 GG als eingeschränktes Grundrecht ausdrücklich zu zitieren. Offenbar war der Gesetzgeber der Auffassung, dass mit der Erhebung und Auswertung von Aktivmeldungen (ohne dass gleichzeitig Telekommunikation stattfindet) nicht in das Telekommunikationsgeheimnis eingegriffen wird. Ob diese Auffassung mit dem Grundgesetz im Einklang steht, wird das Bundesverfassungsgericht zu entscheiden haben, dem eine entsprechende Verfassungsbeschwerde bereits vorliegt. Es ist zu kurz gegriffen, nur die – technisch vermittelte – menschliche Kommunikation und ihre näheren Umstände unter den Schutzbereich des Telekommunikationsgeheimnisses zu fassen. Auch die Kommunikation zwischen Maschinen (Computern) – soweit sie von Menschen initiiert wird oder in ihrem Auftrag erfolgt – fällt in den Schutzbereich des Grundrechts. Anderenfalls wäre nicht verständlich, weshalb der Gesetzgeber für den Einsatz des IMSI-Catchers überhaupt eine gesetzliche Grundlage für erforderlich gehalten hat. Auch die stille SMS (Tarnkappen-SMS, „stealth ping“) darf nur in den Grenzen der Strafprozessordnung zur Ortung von Verdächtigen genutzt werden. Die Frage des Schutzbereichs des Artikels 10 wie auch des einfachgesetzlichen Telekommunikationsge-

11 Sicherheit und Recht auf Privatsphäre für Bürger im Digitalzeitalter nach den Anschlägen des 11. September: Zukunftsgerichteter Überblick, European Commission, Joint Research Centre, Institute for Prospective Technological Studies, July 2003, Deutsche Zusammenfassung unter <http:/www.jrc.es/home/toolbar/whats_new.html>

12 BGBl.2002 I, S. 3018.

heimnisses ist zudem deshalb von wachsender Bedeutung, weil gerade bei der Nutzung des Internets zunehmend intelligente Software-Agenten zum Auffinden von Informationen wie auch zum Abschluss von Verträgen eingesetzt werden.

7. Telekommunikationsnetze sind keine rechtsfreien Räume. Was offline verboten oder strafbar ist, wird online nicht legal. Deshalb muss Kriminalitätsbekämpfung auch grenzüberschreitend in weltweiten Netzen möglich sein. Sie muss sich aber strikt am Grundsatz der Verhältnismäßigkeit orientieren. Der Bundesinnenminister hat mit Recht die revolutionäre Entwicklung des Internet mit der Erfindung der Buchdruckerkunst verglichen. Dieser Vergleich ist auch in anderer Hinsicht treffend: Gibt es Gründe, den Austausch von Informationen online umfassender zu kontrollieren als offline, also in der realen Welt? Ich meine: Nein. Die Vertreter der Sicherheitsbehörden verlangen immer wieder eine Angleichung ihrer Befugnisse im Cyberspace an die Befugnisse in der offline-Welt. Diese Forderung erscheint prinzipiell legitim, rechtfertigt aber keine überschießenden Befugnisse, für die es in der analogen Welt keine Entsprechung gibt. Denn die offline-online-Analogie gilt auch umgekehrt: Was offline erlaubt ist, nämlich die prinzipiell unbeobachtete oder jedenfalls nicht mit zwangsweiser Identifikation verbundene Bewegung, muss auch online im Grundsatz möglich bleiben. Wer ein Buch oder eine Zeitung kauft, muss sich in der realen Welt nicht ausweisen, wenn er bar bezahlt. Eine flächendeckende Überwachung aller Bewegungen und Lebensäußerungen scheidet von Verfassungs wegen selbst dann aus, wenn sie technisch möglich sein oder werden sollte. Die umfassende und anlassunabhängige Registrierung von Abrufen aus dem WorldWideWeb wäre zugleich ein unverhältnismäßiger Eingriff in die Meinungs- und Informationsfreiheit.

   Etwas anderes mag in Chatrooms gelten, an denen sich Ermittler unter den gleichen Bedingungen (also auch unter Pseudonym) wie alle anderen Internet-Nutzer beteiligen können. Die Problematik des *agent provocateur* kann sich hier wie in der realen Welt stellen, ist aber kein genuines Problem des Datenschutzes. Auch gegen eine anlassunabhängige Kontrolle der Informationsangebote im WorldWideWeb, wie sie das Bundeskriminalamt seit einiger Zeit betreibt, sprechen keine prinzipiellen Einwände.

   Kommunikationsnetze würden ihren Charakter dagegen grundlegend negativ verändern und zu regelrechten Plattformen der Verdachtsschöpfung werden, wenn routinemäßig und anlassunabhängig Verkehrsdaten auf Vorrat allein für Zwecke einer eventuellen Nutzung für Zwecke der Gefahrenabwehr oder Strafverfolgung in der Zukunft gespeichert würden. Kein Datenschutzbeauftragter unterstellt den Vertretern der Sicherheitsbehörden, die entsprechende Forderungen erheben, einen Überwachungsstaat errichten zu wollen. Aber der Gesetzgeber sollte keine Befugnisse formulieren, die objektiv über das gebotene Maß hinausschießen.

8. Die Ergebnisse der parallelen Untersuchungen des Max-Planck-Instituts für internationales Strafrecht und der Universität Bielefeld zwingen zu Veränderungen im System der staatlichen Kommunikationsüberwachung. Die Steigerung der Zahl der Ermittlungsverfahren, in denen eine Telekommunikationsüberwachung angeordnet worden ist, zwischen 1990 und 2000 um das Sechsfache, kann nicht allein mit dem Wachstum der Mobilkommunikation erklärt werden. Die Telekommunikationsüberwachung wird immer mehr zur standardmäßigen Ermittlungsmaßnahme („prima ratio“ statt wie von der StPO vorgesehen „ultima ratio“). Das in der Strafprozessordnung vorgesehene Regel-Ausnahme-Verhältnis wird in der Rechtspraxis praktisch in zweifacher Weise auf den Kopf gestellt: Die Überwachung der Telekommunikation wird zum einen vielfach angeordnet, ohne dass ausreichend geprüft worden wäre, ob weniger einschneidende Maßnahmen ebenfalls zum Erfolg führen würden. Zum anderen wird auch der im Gesetz als Ausnahme vorgesehene Eilfall der Anordnung durch die Staatsanwaltschaft (mit richterlicher Bestätigung nur unter bestimmten Voraussetzungen) immer häufiger zum Regelfall. Nur in 17 % der Fälle brachte die Überwachungsmaßnahme zudem einen Ermittlungserfolg, der sich direkt auf den die Telefonüberwachung begründenden Verdacht bezog. 73 % der betroffenen Anschlussinhaberinnen und –inhaber wurden nicht über die Maßnahme unterrichtet.

9. Die vom Bundesinnenminister angekündigte Revision der Telekommunikationsüberwachung sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder folgende Punkte berücksichtigen:[13]

   – die statistische Transparenz der Überwachung muss erhöht[14] und die wissenschaftliche Evaluation ihrer Wirksamkeit muss fortgeführt und erweitert werden; der Gesetzgeber sollte die gesetzlichen Regelungen den Ergebnissen der Evaluation anpassen;

   – der Richtervorbehalt darf als Konsequenz aus der Untersuchung von *Backes* und *Gusy* nicht etwa gelockert, sondern er muss im Gegenteil gestärkt werden;

   – gerade weil die Eilbedürftigkeit der Überwachung immer häufiger, wenn nicht sogar im Regelfall behauptet wird, sollte der Gesetzgeber vorsehen, dass die Ergebnisse von Eilanordnungen der StA nur nach richterlicher Überprüfung verwertet werden dürfen;

   – die Qualität der richterlichen Entscheidungen sollte verbessert werden, indem erhebliche Begründungsmängel zu Beweisverwertungsverboten führen;

13 Entschließung der 66. Konferenz in Leipzig vom 25./26. 9. 2003.

14 Die Bundesregierung hat gegenüber früheren Referentenentwürfen ihre Absicht aufgegeben, die Unternehmensstatistik aus dem TKG zu streichen. Notwendig wäre eine konsolidierte umfassende Statistik-Regelung in der StPO.

- die Aufgaben der Ermittlungsrichter sollten auf wenige Personen konzentriert werden;
- der Straftatenkatalog des § 100 a StPO ist kritisch zu überprüfen, gegebenenfalls zu reduzieren oder durch eine alternative, normenklar geregelte Eingriffsschwelle zu ersetzen;
- die Pflicht zur Benachrichtigung aller bekannten Gesprächsteilnehmer ist zu präzisieren und abzusichern; die Benachrichtigung sollte längerfristig nur mit richterlicher Zustimmung zurückgestellt werden dürfen;
- abgehörte Gespräche zwischen Beschuldigten und Zeugnisverweigerungsberechtigten sollten grundsätzlich nicht verwertet werden dürfen;
- Daten aus Telekommunikationsüberwachungsmaßnahmen müssen gekennzeichnet werden, die hierzu notwendigen technischen Voraussetzungen müssen geschaffen werden;
- die Höchstdauer der Telekommunikationsüberwachung sollte auf zwei Monate reduziert werden;
- PINs und PUKs unterliegen dem Telekommunikationsgeheimnis, auf sie darf deshalb nur unter den gleichen Voraussetzungen zugegriffen werden wie auf Gesprächsinhalte[15];
- eine Zwangsidentifizierung beim Erwerb von prepaid-Handys ist abzulehnen. Zwar hat das Bundesverwaltungsgericht in einer neueren Entscheidung die Auffassung der Datenschutzbeauftragten bestätigt, wonach das geltende Telekommunikationsgesetz keine Rechtsgrundlage für eine Verpflichtung der Anbieter zur Erhebung von Bestandsdaten selbst in den Fällen enthält, in denen der Telekommunikationsdienst vorab bezahlt wird.[16] Der Gesetzgeber sollte aber aus dieser Entscheidung nicht voreilig die Konsequenz ziehen, dass eine entsprechende Verpflichtung „mit einem Federstrich“ zu schaffen ist.[17] Eine zuverlässige Identifikation aller Handy-Nutzer ist auf diese Weise nicht zu erreichen. Die Konferenz der Datenschutzbeauftragten hat betont, dass die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten

15 Die entgegengesetzte Regelung im Entwurf der Bundesregierung für ein Telekommunikationsgesetz (§ 111 Abs. 1 Satz 2) stößt nicht nur auf rechtliche Bedenken, sondern sie führt in der Praxis auch nicht weiter: Da die Netzbetreiber (etwa Mobilfunkanbieter) ebenso wenig wie die Banken bei der Ausgabe von PINs für EC-Karten die rechnergestützt erzeugten und dem Kunden verschlossen übergebenen PINs und PUKs für die SIM-Cards selbst kennen dürfen, können sie sie auch den Strafverfolgungsbehörden nicht zugänglich machen, ohne die Datensicherheit des gesamten Systems in Frage zu stellen.

16 Urteil v. 22. 10. 2003, Az. 6 C 23.02. Dabei hat das Gericht die Grundsätze der Datenvermeidung und der Datensparsamkeit aus dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung abgeleitet.

17 Eine entsprechende Regelung ist in § 109 TKG-E enthalten.

zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen würde. So seien erfahrungsgemäß die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch. Statt der Hintermänner, die zur Vorbereitung von Straftaten häufig Strohleute einsetzen, um aufladbare SIM-Karten zu kaufen, geraten unbescholtene Familienväter in das Visier der Fahnder, wenn sie ihren Kindern derartige Karten schenken wollen und sich zuvor identifizieren müssen.

10. Für die Schaffung präventiv-polizeilicher Befugnisse zur Telekommunikationsüberwachung (geltendes Recht bereits in Thüringen, beschlossen in Niedersachsen, Gesetzentwürfe in Rheinland-Pfalz und Bayern) ist ein Bedarf bisher nicht überzeugend dargelegt worden.[18] Dadurch würde zudem der Anfangsverdacht als Eingriffsvoraussetzung aufgegeben und die Befugnis zu derart schweren Grundrechtseingriffen der staatsanwaltschaftlichen Kontrolle entzogen und noch weiter in das Vorfeld verlagert, ohne dass ein Richtervorbehalt angesichts der verwendeten Blankettbegriffe diesen Kontrollverlust effektiv kompensieren könnte.

11. Angriffe auf Netze, Infrastrukturen und Computer (Computer-Kriminalität) können und müssen sehr viel effektiver als bisher durch eine Erhöhung der Technik-Sicherheit (Produkte, Verfahren) abgewehrt oder erschwert werden. Dazu unternimmt die Europäische Union verstärkte Anstrengungen (Gründung einer Europäischen Agentur für Netzsicherheit – ENISA). Herr Helmbrecht und Herr Brunnstein haben eindrucksvoll die Sicherheitsrisiken beschrieben, die gerade im Internet bestehen („Internet ist Risiko."– Brunnstein) Man sollte nicht die prinzipielle Unsicherheit des Mediums durch ein Übermaß an Überwachung der Nutzerinnen und Nutzer zu kompensieren suchen. Entweder muss die Sicherheit der Infrastruktur entscheidend verbessert oder diese unsichere Infrastruktur darf jedenfalls für bestimmte Zwecke nicht genutzt werden. Als Beispiel sei die Verarbeitung von unverschlüsselten Patientendaten auf Computern mit Internet-Anschluss genannt, die nahezu zwangsläufig zu einer Verletzung der ärztlichen Schweigepflicht führt. Auch das Computerstrafrecht erfüllt eine wichtige ergänzende Funktion, aber es rechtfertigt es nicht, sensitive personenbezogene Daten ohne zureichende Schutzmaßnahmen dem Zugriff Unbefugter aus dem weltweiten Netz auszusetzen.

12. In einem freiheitlichen Rechtsstaat müssen der Schutz der Grundrechte, also auch des Rechts auf vertrauliche Kommunikation die Regel und ihre Einschränkung die begründungsbedürftige Ausnahme im Einzelfall bleiben. Der Staat darf nicht allein die Tatsache, dass jemand Kommunikationsnetze

18 Aufschlussreich insofern das Protokoll der Anhörung zum Thema „Präventive Telekommunikationsüberwachung" in der gemeinsamen Sitzung der Ausschüsse für Kommunale Fragen und Innere Sicherheit sowie für Verfassungs-, Rechts- und Parlamentsfragen des Bayerischen Landtages am 1. 7. 2003 (Wortprotokoll).

nutzt, zum Anlass dafür nehmen, seine Bewegungen und Äußerungen umfassend zu registrieren, und so jeden, der – aus legitimen Gründen – unbeobachtet kommunizieren will, zur Technikabstinenz zwingen. Der Verlust an Freiheit wäre zugleich ein Verlust an Sicherheit, nämlich der Sicherheit Unverdächtiger, Telekommunikationsnetze unregistriert nutzen zu können. Es darf nicht dazu kommen, dass Informations- und Kommunikationsnetze prinzipiell überwachungsgeneigt sind, und nur noch die persönliche Kommunikation (abgesehen vom Großen Lauschangriff) überwachungsfrei möglich ist.

Zurück zu Benjamin Franklin: Weil die Menschen sowohl Sicherheit als auch Freiheit „verdienen", sollten sie nicht wesentliche Freiheiten für „ein wenig vorübergehende Sicherheit" aufgeben. Sicherheit ist stets nur vorübergehend, während der Verlust von Freiheit sich kaum jemals revidieren lässt.

Rechtsfreie Räume zulassen – die Anarchie im Netz akzeptieren?

– Ein Streitgespräch –

Die Teilnehmer des abschließenden Streitgesprächs *(von links)*:
Jürgen Schütte von der Bezirksregierung Düsseldorf, Franz-Hellmut Schürholz vom LKA Baden-Württemberg, Diskussionsleiter Ulrich Kienzle, Andy Müller-Maguhn vom Chaos Computer Club und Axel Kossel von der Zeitschrift c't

Herr Kienzle:

„Rechtsfreie Räume zulassen – die Anarchie im Netz akzeptieren?" - das ist die Frage, die wir uns hier stellen. Bei der Recherche zu diesem Thema bin auf ein paar verstörende Entdeckungen gestoßen. Der Bund Deutscher Kriminalbeamter behauptet forsch: „Das Internet ist ein rechtsfreier Raum. Die Polizei hat den Kampf gegen die Internetkriminalität längst verloren." Die Zeitschrift PC Tipp beklagt dagegen das Sterben der Internetanarchie. Zwei total unterschiedliche Positionen. Und der PC Tipp gibt den Kampf gegen die Regulierung des Internets verloren. Konzerne und Staaten hätten längst die Macht im Internet übernommen, meine Damen und Herren. Beide reden von der gleichen Sache. Die Frage ist: Wer hat Recht? Das möchte ich, bevor wir in die Diskussion einsteigen, mit meinen Mitdiskutanten klären. Rechts von mir sitzt Franz Helmut Schürholz, Präsident des Landeskriminalamts Baden-Württemberg. Daneben Andy Müller-Maguhn vom Chaos Computer Club Berlin, dann Jürgen Schütte von der Bezirksregierung Düsseldorf. Die ist ja dadurch bekannt geworden, dass sie gelegentlich zuschlägt

und sich nicht alles gefallen lässt. Und dann Axel Kossel, leitender Redakteur der Computerzeitschrift CT.

Wer hat Recht, Herr Schürholz: Ihre Kollegen von der Kripo oder PC Tipp?

Herr Schürholz:

Ich denke, keiner von beiden. Was Polizei und Justiz betrifft, sind wir dabei, in einer großen Nachholoffensive Kompetenz zu erwerben, Ausstattung zu verbessern, Instrumentarien zu verschärfen, um unseren gesetzlichen Auftrag, den wir auch im sozialen Raum Internet haben, zu erfüllen.

Herr Kienzle:

Herr Schürholz, habe ich das richtig verstanden? Nachholoffensive? Das heißt, Sie haben was verpasst.

Herr Schürholz:

Wir sind immer ein Stück weit reaktiv. Reaktiv, weil wir ja keinen Überwachungsstaat haben wollen und daher in der Regel auf unser kriminelles Gegenüber reagieren. Insoweit haben wir es immer mit einer Phasenverschiebung in unseren Reaktionen zu tun.

Herr Kienzle:

Sind Sie denn auf Augenhöhe mit dem kriminellen Milieu im Internet?

Herr Schürholz:

Nein, das sind wir noch nicht.

Herr Kienzle:

Das war ein sehr freimütiges Geständnis, meine Damen und Herren. Das erste Geständnis heute. Ich begrüße das heftig. Eine Frage dann an Herrn Müller-Maguhn. Es geht ja immer noch um die Frage, Anarchie im Internet? Stirbt die, oder ist die wichtig und richtig?

Herr Müller-Maguhn:

Das Internet ist ja zunächst einmal eine Vernetzung von Netzen und bringt natürlich ein neues Medienparadigma mit sich. Früher hatte man bei Medien eine eingeschränkte Anzahl von Sendern, die man mit Landesmedienanstalten oder Pressegesetzen oder Ähnlichem behandeln konnte. Und jetzt ist jeder Teilnehmer am Kommunikationsgeschehen, auch möglicher Sender und das auch noch transnational.

Das, was sie als Anarchie oder rechtsfreie Räume attestieren, sind in Wirklichkeit nur unterschiedliche kulturelle Vorstellungen, die sich auch in gesetzlichen Vorschriften widerspiegeln – allerdings national eben sehr unterschiedlich geprägt. Der nordamerikanische Verfassungsgrundsatz des First Amendment, also dem

Verfassungsgrundsatz auf freie Rede, steht eben den hierzulande vorhandenen Einschränkungen im Bezug auf rechtsextremistische bzw. menschenverachtende Äußerungen aufgrund der deutschen Geschichte entgegen. Trotzdem ist das Ergebnis im Internet kein rechtsfreier Raum, sondern ein Raum, wo nach den Vorstellungen von amerikanischen Regierungsvertretern die amerikanischen Gesetze und nach den Vorstellungen von deutschen Regierungsvertretern die deutschen Gesetze gelten sollen.

Herr Kienzle:

Einfach eine Nachfrage zu der Frage, die ich anfangs gestellt habe. Der Bund Deutscher Kriminalbeamter ist ja gelegentlich vorlaut. Ist denn der Satz, den ich da im Internet gefunden habe, richtig, dass die Polizei den Kampf gegen die Internetkriminalität längst verloren hat?

Herr Müller-Maguhn:

Ich befürchte, das hängt davon ab, wie Sie diese Kriminalität definieren. Natürlich gibt es bestimmte Sachen, die man in diesem Netz tun kann. Die können Sie im wirklichen Leben nicht machen. Bloß, ob die illegal sind, darüber werden wir uns unterhalten müssen. Beispielsweise bei dem Vorhaben, wo wir uns mit der Bezirksregierung Düsseldorf angelegt haben, da sagen wir ja nicht, dass es nicht illegal sein sollte, in Deutschland solche Äußerungen zu tätigen, sondern wir sagen einfach: Der Staat hat doch kein Recht, ein Empfangsverbot zu deklarieren. Es kann doch nicht angehen, dass die deutsche Regierung den Bürgern vorschreibt, welche „Feindsender" sie hören darf und welche nicht. Das hatten wir ja auch schon einmal. Das ist ja nicht die historische Wirklichkeit, die wir zurückerobern wollen, sondern wir wollen schön differenzieren und die Dinge auseinander halten. Deswegen kann ich jetzt nicht so platt sagen: Ja, ist es jetzt ein rechtsfreier Raum oder nicht. Sondern es sind wirklich viele unterschiedliche Schichten von Angelegenheiten, die da aufeinandertreffen. Wenn Sie jetzt beispielsweise den Anspruch haben, Urheberrechte durchzusetzen und jedwede Äußerung, die mit deutschem Recht nicht in Einklang zu bringen ist, rechtlich zu bekämpfen, na dann wünsche ich Ihnen natürlich viel Spaß beim Kampf gegen die Windmühlen. Sie wissen ja selber, wohin das ausartet. Die drehen sich dann besonders schön. Bloß, ob das Sinn macht, ist eine andere Frage. Natürlich muss man da auch wirklich regeln, wo die Dinge sind, die man aus gesellschaftlicher Sicht, sozusagen an Kriminalität, nicht akzeptieren kann, wo man gegen diese vorgehen kann. Und da gibt es in der Regel auch Mittel. Das Internet ist immer noch nur ein Kommunikationsnetz, was Menschen miteinander vernetzt. Und die halten sich in Rechtsräumen, in so genannten Jurisdiktionen auf. Aber die Menschen halten sich eben immer nur an die Gesetze des Landes, in dem sie sich befinden, – wenn überhaupt.

Herr Kienzle:

Es wurde das Stichwort „Don Quichotte“ geliefert. Deshalb frage ich Herrn Schütte: Fühlen Sie sich als solcher, wenn Sie im Internet zuschlagen? Sie haben ja mehrfach gesagt: Wir können das nicht so akzeptieren und einfach so laufen lassen. Die Frage an Sie: War das erfolgreich?

Herr Schütte:

Ob es erfolgreich war, kann man, glaube ich, noch nicht abschätzen. „Don Quichotte“ würde ich auch nicht sagen. Man muss verstehen, in welchem Umfeld wir uns befinden, weswegen ich noch einmal an Ihre erste Frage anknüpfe, ob Internet rechtsfreier Raum ist. Faktisch ja, rechtlich natürlich in Deutschland zumindest eindeutig ein Nein. Das ist der Widerspruch. Wir haben es im Internet mit einem globalen Medium zu tun, was keine nationalen Grenzen kennt, haben aber eine nationale Rechtsordnung. Das ist gerade bei rechtsextremen Internetinhalten der Widerspruch. Wir haben es mit Straftaten zu tun, konkret mit rechtsextremen Straftaten, mit Propagandastraftaten, die im Internet verbreitet werden. Ich denke, niemand zweifelt daran, dass dieses auch im Internet strafbar ist. Denn es steht nicht im Strafgesetzbuch, dass Volksverhetzung oder das Verwenden verfassungswidriger Zeichen überall verboten ist, nur im Internet dagegen erlaubt. Das steht jedenfalls im Strafgesetzbuch nicht drin. Also ganz eindeutig: In Deutschland unterliegt auch das Internet dem geltenden Recht. Die Frage ist nur, wie man dieses Recht durchsetzen kann? Und das hat die Bezirksregierung Düsseldorf als zuständige Aufsichtsbehörde für das gesamte Land Nordrhein-Westfalen versucht und erreicht, dass die Accessprovider diese beiden rechtsextremen, strafbaren Internetinhalte, um die es geht, in Nordrhein-Westfalen zumindest, gesperrt haben. Das heißt, ohne große technische Fachkenntnis dürften in Nordrhein-Westfalen die Nutzer den Zugang zu diesen Inhalten nicht mehr haben. Die Bezirksregierung bemüht sich deswegen für Nordrhein-Westfalen, den Taterfolg dieser Straftaten zu vereiteln.

Herr Kienzle:

Sie haben gesagt: Wir haben es versucht. Waren Sie auch richtig erfolgreich? Sie haben ja selber gerade zugegeben, dass ein geschickter Internetnutzer an diese Information nach wie vor herankommen kann.

Herr Schütte:

Ich will das gerne ergänzen. Natürlich kann ein geschickter Internetnutzer mit technischen Kenntnissen da rankommen. Nur ich denke, man muss abstellen auf den Durchschnittsnutzer. Das Oberverwaltungsgericht in Nordrhein-Westfalen, das unsere Verfügung im einstweiligen Rechtsschutzverfahren bestätigt hat, hat gesagt: „Jawohl. Das reicht auch aus für die Geeignetheit einer solchen Maßnahme.“ Problematisch ist natürlich weiterhin, dass wir in Nordrhein-Westfalen als einzige Aufsichtsbehörde so gehandelt haben. Ein Internetnutzer kann

sich natürlich auch einem Accessprovider außerhalb Nordrhein-Westfalens, also in einem anderen Bundesland oder in Europa oder sonst wo in der Welt anschließen. Dann kann er natürlich wieder an diese Inhalte herankommen. Also wirksam, wenn Sie mich fragen, wird diese Maßnahme nur, wenn viele Aufsichtsbehörden so handeln wie wir. Wir als Aufsichtsbehörde unterliegen dem Mediendienststaatsvertrag. Dem unterliegen alle anderen Bundesländer auch. Und wir finden es schon einigermaßen unverständlich, dass die anderen Bundesländer bisher nicht das getan haben, was das Gesetz vorsieht.

Herr Kienzle:

Das ist ein erstaunlicher Vorwurf, meine Damen und Herren. Den wollen wir festhalten. Aber ich möchte noch einmal Herrn Kossel fragen, der ja eine weitgehend interessante These hat. Er sagt: Der Rechtsstaat unterscheidet sich vom totalitären System dadurch, dass er Anarchie bis zu einem gewissen Grad zulässt. Wie meinen Sie das?

Herr Kossel:

Ich denke, der Rechtsstaat ist eben in der Lage, durch Bildung und durch gesellschaftliche Formung auf eine totale juristische, in diesem Fall Abhörkontrolle seiner Bürger zu verzichten. Das ist eigentlich eine Aufgabe, eine Befähigung, die dem Bürger vermittelt werden muss, das muss heute in den Schulen passieren. Das muss ganz besonders für die nächsten Generationen passieren, nämlich die Menschen zu befähigen, mit den Informationen im Netz, die Sie finden, umzugehen: Und letztlich geht es doch nicht an, dass wir solche Informationen, die wir hier nicht haben, bekämpfen, indem wir sie unter den Teppich kehren, indem wir einfach sagen: Wir verstecken sie im deutschen Internet. Dieses Verstecken ist, wie auch schon angesprochen wurde, sowieso nur eine oberflächliche Reaktion. Wer sich auskennt, kommt sowieso an diese Informationen ran. Die Kreise, die wirklich solche Informationen suchen – und das sind die gefährlichen Kreise –, kommen an diese Information ran. Nur, weil wir sagen, dass wir beispielsweise den unbedarften Jugendlichen vor diesen Informationen schützen, bedeutet das keine wirklich gute Gegenmaßnahme. Viel besser wäre es, wenn wir unsere Jugend dazu befähigen würden, selbst diese Informationen als böse oder schlecht einzuschätzen und gar nicht erst danach im Internet suchten.

Herr Kienzle:

Das ist der Glaube an die Erziehung, meine Damen und Herren. Ich weiß nicht, ob wir uns darauf nach PISA so verlassen sollten. Da habe ich meine Zweifel. Aber noch mal die Nachfrage. Das heißt doch: bestimmte rechtsfreie Räume zulassen.

Herr Kossel:

Wir können bestimmte rechtsfreie Räume nicht zulassen, solange sie innerhalb unserer Rechtsprechung liegen. Es ist die Aufgabe des Staates, dagegen vorzuge-

hen. Aber wir können nicht sagen, dass wir – bis hin zur Zensur – unsere eigenen Rechtsvorstellungen in einem weltweiten Netz mit Gewalt durchsetzen.

Herr Kienzle:

Was meinen Sie „mit Gewalt durchsetzen“? Ist das im Internet überhaupt möglich? Nach Ihrem Verständnis ist es ja gar nicht möglich, oder? Habe ich Sie richtig oder falsch verstanden?

Herr Kossel:

Na ja, für mich ist es eine Art Gewaltakt, wenn man sagt, dass man filtert. Nur, solche Gewalt erzeugt natürlich irgendwo Gegengewalt. Das heißt, die andere Seite fängt dann an, diese Filtermaßnahmen auszutricksen. Die Internetseiten tauchen ständig irgendwo anders auf. Wenn das jetzt in ganz Deutschland so weitergeht und bestimmte Seiten gesperrt werden, dann fällt das ja irgendwo auch im Ausland auf. Dann werden diese Seiten herumgeschoben. Und dann können sich ganze Behörden damit beschäftigen, täglich die Filtersysteme auf dem aktuellen Stand zu halten. Ich glaube, diese Arbeit möchte sich niemand ans Bein binden.

Herr Kienzle:

Herr Schürholz. Die Arbeit haben Sie.

Herr Schürholz:

Ja, und diese Arbeit scheuen wir auch nicht. Wir sind der Meinung, dass neben den Möglichkeiten, die die Medienaufsicht hat, natürlich die Ermittlungen ihren Part spielen müssen. Das heißt für mich: Wenn deutsche Rechtsextremisten ins Ausland gehen, um auf dortigen Servern ihre Botschaften unterzubringen, um sie vermeintlich strafrechtlich ohne Folgen hier loszuwerden, dann müssen wir diese deutschen Tatverdächtigen aufspüren und sanktionieren. Und genau dieses tun wir auch.

Herr Kienzle:

Wie erfolgreich sind Sie denn dabei? Haben Sie denn Erfolgserlebnisse, die Sie uns mitteilen können?

Herr Schürholz:

In vielen Fällen ist es uns gelungen, diese Tatverdächtigen zu ermitteln. Manchmal spielen uns die unzulänglichen Rechtsinstrumente einen Streich dabei. Zum Beispiel: Wenn wir ermittelt haben, über welchen deutschen Provider der deutsche Tatverdächtige an den ausländischen Server gekommen ist, wollen wir die deutsche Adresse dieses Mannes feststellen. Das scheitert aber, wenn der deutsche Internetprovider die entsprechenden Verbindungsdaten gelöscht hat. Hier braucht es eben eine Rechtsänderung. Das heißt, dass die Verbindungsdaten für Zwecke der Strafverfolgung zwölf Monate aufbewahrt werden; dann könnten wir in unseren Ermittlungen und nachher auch in der strafrechtlichen Sanktion er-

folgreich sein. Dann blieben deutsche Straftäter eben nicht mehr straflos, wenn sie ihre kriminellen Inhalte über das Ausland verbreiten.

Herr Kienzle:

Nur eine Lernfrage dazu. Wer verhindert denn, dass es politisch zu einer Lösung in dieser Frage kommt? Gibt es da aus einem bestimmten Milieu Widerstand dagegen? Spüren Sie den und können Sie den auch benennen?

Herr Schürholz:

Es gibt eben leider bisher keine bundesrechtliche Regelung, die die Internetserviceprovider verpflichtet, eine entsprechende Datenart

a) zu erheben,
b) zu speichern über einen Zeitraum, der für die Strafverfolgung ausreichend Zeit lässt – aus unser Sicht zwölf Monate.

Da ist der Bundesgesetzgeber in der Pflicht. Und dieser Pflicht ist er bisher noch nicht nachgekommen, obwohl die Sicherheitsbehörden deutlich gesagt haben, was sie brauchen.

Herr Kienzle:

Das wäre ja ein Vorwurf an den Bundesinnenminister. Der hat ja am Dienstag hier gesagt: Wir sind eigentlich sehr gut aufgestellt. Herr Schütte, ist das denn so?

Herr Schütte:

Ich sage mal so: Ja und Nein. Ich wollte aber auf die Problematik eingehen, die Herr Schürholz eingebracht hat.

Herr Kienzle:

Herr Schütte, Entschuldigung, dass ich da noch mal nachhake, weil: Das ist ja doch wohl eine essenzielle Frage. Ein „Jein“ akzeptiere ich als Antwort einfach nicht. Sie müssen sich schon klarer ausdrücken. Ist das denn die Crux, die Sie im Augenblick haben? Oder gibt es Länderregelungen, die das ermöglichen, was der Bund im Augenblick offensichtlich noch nicht ermöglicht?

Herr Schütte:

Herr Kienzle, ich wollte keinem zu nahe treten.

Herr Kienzle:

Treten Sie ruhig nahe. Jetzt sind wir ja ganz unter uns.

Herr Schütte:

Vor dem Hintergrund des Medienordnungsrechts und der Rechtsgrundlagen, von denen wir Gebrauch gemacht haben, halte ich die rechtlichen Grundlagen für aus-

reichend. Und genau das wollte ich gerade darstellen. Wir stehen vor dem Hintergrund des Rechtsextremismus' vor folgendem Sachverhalt: Ein deutscher Rechtsextremist, der illegale strafbare Inhalte ins Internet eingeben will und verbreiten will, tut das natürlich nicht mit einer deutschen Domänennummer über einen deutschen Provider. Denn dann wäre er sofort fassbar und könnte von der Polizei sofort verfolgt werden. Er tut dies gewöhnlich – und das sind 80 bis 90 % der Fälle – über amerikanische Serviceprovider. Und zwar lanciert er seine Inhalte dort anonym hin. Man kann nicht nachverfolgen, jedenfalls mit legalen Mitteln bisher nicht, von wem dieser Inhalt stammt. Von diesem amerikanischen Serviceprovider, der dort durch ein anderes Verständnis der Meinungsfreiheit, durch das First Amendment geschützt ist, werden diese Inhalte dann weltweit verbreitet. Und mangels irgendwelcher internationaler Abkommen erscheinen diese Inhalte dann so hier, als hätte dieser Rechtsextremist diese Inhalte direkt hier verbreitet. Und das ist die Crux, vor der wir stehen. Das Strafrecht kommt nicht mit, jedenfalls nicht mit den bisherigen Mitteln. Das Strafrecht bietet keine Möglichkeiten, um die wirklich dahinterstehenden Täter zu ermitteln. Die Serviceprovider, die in den USA sitzen, sind rechtlich nicht belangbar. Sie werden ausdrücklich durch die amerikanische Verfassung geschützt. Also bleibt nur der dritte Weg. Und von dem hat eben die Bezirksregierung Düsseldorf für Nordrhein-Westfalen Gebrauch gemacht. Dieser Weg ist, die Accessprovider, die hier den Nutzern den Zugang ermöglichen, zur Sperrung in Anspruch zu nehmen. Das haben wir getan. Gäbe es die Accessproviderhaftung nicht, dann entstünde wirklich in Deutschland auch theoretisch ein rechtsfreier Raum. Es gäbe keine Möglichkeit mehr, gegen diese Inhalte vorzugehen. Nur mithilfe der Accessproviderhaftung wird sozusagen diese Haftungslücke geschlossen. Ich denke, das ist die – ich darf das mal bescheiden sagen – besondere Bedeutung des Medienordnungsrechts, die ich eben nicht so hervorheben wollte.

Herr Kienzle:

Herr Müller-Maguhn, ist das denn, was Herr Schütte gerade beschrieben hat, ein richtiger Weg? Ist das ein erfolgreicher Weg? Ist das wirklich ein Weg, der dazu führt, dass wir tatsächlich weniger rechtsradikale Propaganda im Internet haben werden in Deutschland?

Herr Müller-Maguhn:

Nein, ich glaube, das ist ein ziemlicher Unsinn, weil es vor allem auf der Annahme beruht, dass wir es hier mit Leuten zu tun haben, die sich an Gesetze halten. Wenn sich jemand tatsächlich im rechtsextremistischen Milieu bewegt und an derartigen Seiten Interesse hat, dann scheut er ja auch nicht den Aufwand, um mit ein paar Tastaturgriffen den Versuch, den Abruf dieser Seiten zu verhindern, zu umgehen. Das ist einfach technisch viel zu einfach. Die Maßnahmen erzeugen sozusagen zum einen ein gefährliches Irrbild, nämlich, man könne mit diesen Mitteln tatsächlich den Abruf dieser Seiten verhindern, was schlicht nicht der Fall ist. Das heißt, sie suggerieren sozusagen, dass man dagegen etwas tut. In Wirklichkeit ist

das aber Populismus. Und zum anderen lenken sie halt ein bisschen auch davon ab, dass die eigentlich Sache ja die ist: Rechtsfreie Räume kann ich auch so nicht akzeptieren als Regelung. Freiherr von Knigge hat vor 300 Jahren auch schon gesagt: Der Planet ist groß genug, dass eine Menge Narren nebeneinander darauf Platz haben. Ich denke, so muss man das auch ein bisschen sehen. Es geht ja auch um die gesellschaftliche Frage. Da ist beispielsweise ein Jugendlicher. Und der setzt sich an das Internet und kommt jetzt auf einmal an einen Inhalt heran über dieses Medium, die eigentlich in der Brief- und in der Papierwelt verboten und nicht am Kiosk erhältlich sind. Der liest jetzt irgendwelche Sachen. Und dann rennt er zur nächsten Tankstelle, kauft sich einen Benzinkanister und zündet oder versucht irgendwelche Asylbewerberheime anzuzünden. Da ist doch nicht nur die Frage: Was hat er da gelesen und wie kann man verhindern, dass er es lesen kann? Sondern, was hatte der denn eigentlich vorher im Kopf? Mit was für einer Mentalität geht er mit diesen Inhalten um, welche gesellschaftliche Zustände prasseln auf ihn ein?

Herr Kienzle:

Das finde ich einen ganz wichtigen Punkt. Sie unterstellen, wenn ich Sie richtig verstehe, dass die Jugendlichen cleverer sind als die Polizisten.

Herr Müller-Maguhn:

Das ist doch offensichtlich. Wenn es um den Umgang mit diesen Medien geht, ist das ja eine generationsbedingte Angelegenheit. Ich meine, einige von Ihnen, das ist kein Vorwurf, sind mit dem Radio großgeworden. Aber andere sind mindestens mit dem Telefon, wenn nicht mit dem Internet schon zur Welt gekommen. Und natürlich ist da eine andere Selbstverständlichkeit im Umgang mit Information. Dies bestätigt auch die Filterungsfähigkeit des Einzelnen. Wir sagen ja: Die Filterung hat im Endgerät stattzufinden. Wenn Eltern ihre Kinder vor der Wahrnehmung pornographischer Bilder oder Ähnlichem schützen wollen und dagegen etwas tun: Das ist völlig in Ordnung. Aber die Frage ist ja: Wie verhält sich das gesellschaftlich? Wie bringt man Jugendliche dazu, wenn sie zum Beispiel Dinge sehen, die ihr soziales Wahrnehmungsvermögen stören, dass sie darüber reden. Das ist das Entscheidende. Das heißt, da geht es viel um Elternaufgabe. Es besteht für mich ein gefährlicher Irrglaube, der Staat könne durch eine pauschale Maßnahme alle beschützen, und dann ist alles gut. Und dann denken die Eltern: Das ist ja prima. Wir sitzen in Düsseldorf, die Bezirksregierung macht das schon. Wir können unser Kind ganz ungeschützt vor das Internet setzen. Und das ist eben gerade auch gefährlich, weil: Diese Maßnahme ist einfach ein Witz, einfach nur technisch gesehen ein Witz. Und wie gesagt, derjenige, der an diese Inhalte heranwill, der scheut auch nicht den Aufwand. Das ist so wie bei der Verschlüsselungsdiskussion auch.

Herr Kienzle:

Ich würde gerne die These von Ihnen aufnehmen. Wenn ich das journalistisch übersetze, dann ist das ja, was Sie unterstellen, so eine Art polizeiliche oder bürokratische Selbstbefriedigung, die da betrieben wird, in dem Sie den Eindruck erwecken, diese Maßnahme könne tatsächlich schützen. Herr Schütte, der Vorwurf geht an Sie.

Herr Schütte:

Ja, ich kenne den Vorwurf. Natürlich, das habe ich eben schon gesagt, sind diese technischen Sperrmöglichkeiten, die es bisher gibt – DNS-Sperrung, PROXI-Sperrung, und wie sie sich immer nennen – bisher alle umgehbar. Nur, wenn man sich die leichteste Sperrmöglichkeit einmal ansieht, diese so genannte DNS-Sperrung, bei der der Domainname nicht mehr in die richtige IP-Nummer übersetzt wird, weil man einen anderen Domainnameserver anwählen kann, dann muss man erst einmal wissen, wie man das am Computer macht. Man muss eine neun- oder zwölfstellige andere Zahlenkombination kennen. Die kann man zwar auch irgendwo erfahren. Nur, der wesentliche Punkt bei dieser Argumentation ist – und das sieht Herr Müller-Maguhn falsch –, dass da heute nicht mehr Internetexperten oder technische Experten sitzen, die das Internet nutzen, sondern der gewöhnliche Mann, die gewöhnliche Frau, die ziemlich wenig technisches Verständnis haben. Und die werden sich keine große Mühe geben und werden es auch nicht können, diese technischen Dinge zu bewerkstelligen. Aber zum Kernsatz: Herr Müller-Maguhn hat gesagt: „Die Filterung muss am Endgerät stattfinden." Gut, es gibt Filterprogramme, das weiß heute jeder, nur, Herr Müller-Maguhn bestreitet damit etwas ganz Wesentliches, nämlich die staatliche Schutzpflicht. Wir denken, es gibt auch eine staatliche Schutzpflicht. Die ist niedergelegt im Mediendienststaatsvertrag, Jugendmedienstaatsvertrag und auch in Artikel 1 des Grundgesetzes, in dem es heißt: Der Schutz der Menschenwürde ist staatliche Pflicht. Der Staat kann sicht nicht entziehen und kann zugucken, was da im Internet passiert. Wir können nicht Herrn Spiegel vom Zentralrat der Juden oder jüdischen Mitbürgern und den Ausländern sagen: Bitte, da gibt es zwar KZ-Spiele und irgendwelche ausländerfeindlichen Spiele, die Euch an Bäumen aufhängen. Aber die Zuschauer oder die Nutzer sind schon bewusst genug und werden solche Inhalte nicht ernst nehmen. Ich denke, so können wir mit gesellschaftlichen Minderheiten, die im Internet diskriminiert werden, nicht umgehen. Der Staat hat eine Pflicht und kann sich nicht aus der Affäre ziehen.

Herr Kienzle:

Noch einmal nachgefragt: Herr Kossel, ist es eine Illusion, was Herr Müller-Maguhn hier gesagt hat, nämlich zu glauben, dass dieser Schutz möglich ist?

Herr Kossel:

Ja, also dieses Konzept, was Herr Schütte eben beschrieben hat, beunruhigt mich etwas. Wenn ich es richtig verstanden habe, dann ist diese Filtermöglichkeit dazu da, die Dummen zu schützen und die Schlauen, die sich mit dem Internet auskennen, die können weitermachen was sie wollen. Das kann ja irgendwie nicht das Ziel des Staates sein. Ich möchte einmal kurz technisch werden, was diesen Schutz angeht: Sie können heute beispielsweise ausweichen über einen so genannten PROXI-Server, einen offenen PROXI irgendwo im Ausland, und die Seiten dann abrufen. Dafür gibt es Softwarepakete, die das für Sie übernehmen, die diese PROXIs automatisch einbauen. Da müssen Sie technisch nicht versiert sein. Dann stellen Sie die Anfrage oder rufen die Seite nicht mehr direkt von dem Server ab, sondern rufen diese von einem anderen Server ab, der für Sie die Seiten holt. Das heißt, wenn ich jetzt den Schutz verfeinern möchte, muss ich auch diese so genannten offenen PROXIs ebenfalls sperren, über die aber jemand anderes vielleicht ganz legale Daten holen möchte. Als Nächstes gibt es Suchmaschinen, die im Ausland betrieben werden. Über die ich kann ich Seiten suchen. Ein bekanntes Beispiel ist Google. Da ist ein Archiv, wo die letzte Version dieser Seite abgelegt ist. Wenn ich nun über ein Stichwort eine Neonaziseite im Ausland finde und dann auf Archiv klicke, dann bekomme ich den Inhalt nicht von dieser Seite geliefert, sondern von der Suchmaschine. Auch kein sehr schwieriger Vorgang. Das heißt, ich muss dann die Archive dieser ausländischen Suchmaschine ebenfalls sperren. Und so komme ich immer weiter. Wenn ich wirklich diesem Ansatz folgen will, ich möchte den Bürger schützen und ich möchte natürlich nicht nur die Dümmsten der Bürger schützen, sondern ich möchte eigentlich alle Bürger schützen, dann muss ich immer mehr sperren und mehr sperren. Dann kommen noch weitere Interessengruppen dazu, wie zum Beispiel die IFPI, die die Rechte der Musikindustrie verwaltet. Die hatte diese Idee mit der Filterung nämlich schon vor der Bezirksregierung in Düsseldorf. Die hatte schon Versuche und Tests gemacht. Die möchten gerne eine Filtersystem entwickeln oder installieren, – entwickelt ist es eigentlich schon –, das Ihnen den Zugriff auf Musikdateien oder Videos im Ausland sperrt, die eben illegal kopiert wurden. Da ist also der Ansatz ein anderer. Es geht nicht um Neonaziinhalte, sondern es geht um die Interessen einer Industrie. Und die IFPI möchte am liebsten diese Filterlisten selbst verwalten, weil es dann natürlich am schnellsten geht. Als Nächstes kommen wir natürlich in den Bereich Kinderpornographie. Auch da müssen wir dann anfangen zu filtern. Die Gefahr, die ich in dieser Idee sehe – ich meine, Herr Schütte bezeichnete es ja auch selber als Demonstration, dass es technisch möglich ist und als einen ersten Schritt –,und wenn wir diesen Weg weitergehen, dann kommen wir dahin, dass wir immer mehr filtern, immer mehr filtern. Und irgendwann können wir uns wirklich dem Zensurvorwurf nicht mehr entziehen.

Herr Kienzle:

Das ist ein sehr massiver Vorwurf, Herr Schürholz. Nur die Dummen können Sie eigentlich schützen. Wie sehen Sie das?

Herr Schürholz:

Ich denke, wir müssen den staatlichen Schutzauftrag so weit wahrnehmen, wie irgendmöglich. Deshalb meine ich, müssen eben beide Wege gegangen werden. Die Aufsichtsrechte, die man nach den Mediengesetzen hat, müssen wir nutzen, um einen Erfolg, den unser Recht nicht will, tatsächlich bei uns auch nicht eintreten zu lassen. Und wir müssen daneben den anderen Weg gehen, dass nämlich die Polizei stärker im Internet präsent ist, dass sie sich kümmert um das, was in diesem sozialen Raum tatsächlich geschieht. Und dies macht die Polizei bisher auf sehr schmaler personeller Basis. Die verdienstvollen Pioniere in diesem Bereich, nämlich das Bundeskriminalamt und das Land Bayern, machen das mit etwa vierzig Mitarbeitern. Das ist bezogen auf das anlassunabhängige Recherchieren im Internet sehr, sehr wenig. Alles Übrige wird nur auf konkreten Anlass hin – sprich: auf eine Anzeige, auf einen Hinweis hin – aufgenommen. Das ist bezogen auf eine Präsenz der Polizei, die wirksam Gefahren abwehren und begangene Straftaten aufklären und zur strafrechtlichen Aburteilung bringen will, zu wenig.

Herr Kienzle:

Herr Schürholz, darf ich an dem Punkt nachhaken, Denn das, was Sie gerade eben gesagt haben, ist ja ziemlich desillusionierend. Internetstreifen: Das klingt ja wahnsinnig schön, ist auch zum Verkaufen für die Kollegen von der Pressestelle des BKA eine tolle Geschichte. Das klingt irgendwie toll. Aber Sie haben ja selber die Zahlen genannt. Bei der Tatsache, dass es täglich allein ca. 8.000.000.000 E-Mails gibt, stelle ich mir es sehr schwer vor, da an kriminelle Geschichten heranzukommen. Sie haben ja jetzt einen Fall, der besonders spektakulär ist: der Kannibale von Rothenburg. Das ist ja offensichtlich durch eine solche Internetstreife wirklich ans Licht gekommen. In gleicher Weise würde ich gerne einmal über Kriminalität und Erfolge in dieser Runde sprechen. Welche Erfolge haben Sie denn? Sind die denn wirklich sichtbar, so wie das in der realen Welt ist? Ist das fest zu machen in Zahlen? Ist es fest zu machen an Geld? Ist es festmachbar, so dass es die Öffentlichkeit beeindrucken kann?

Herr Schürholz:

Ich denke, wir haben in einigen großen Ermittlungsverfahren bewiesen, dass wir zum Beispiel gegen Kinderpornografie im Internet wirksam ermitteln können. In mehreren Verfahren, die in den Ländern und im Bundeskriminalamt geführt worden sind, haben wir nicht wenige Organisatoren von Internetforen namhaft gemacht. In diesen geschlossenen Foren ließen die Organisatoren nur Personen zu, die ihnen vertrauenswürdig erschienen. Und dort wurden dann in einem geschützten Raum in großem Umfang kinderpornografische Bilder und Botschaften ausgetauscht.

Allein in einem Verfahren bei uns haben wir gegen die Mitglieder dieser kriminellen Bande – als solche wurden sie nämlich auch verurteilt – mehrjährige Freiheitsstrafen erwirken und damit insgesamt etwa 130 einschlägige Foren im Internet in einem einzigen Verfahren dichtmachen und die Urheber und Organisatoren dafür hinter Gitter bringen können. Das ist im Interesse der missbrauchten Kinder, die ja hinter einer solchen Realität stehen, doch ein sehr, sehr wirksamer und ermutigender Erfolg. Drei, vier weitere Verfahren dieser Größenordnung sind in den letzten Jahren national und international geführt worden mit teilweise über zwölf Monaten Ermittlungsdauer. Aber am Ende stand die Entdeckung und Sanktionierung eines sehr weit reichenden Rings von Vertreibern von Kinderpornografie im Internet und am Ende standen auch harte Strafen. Das ist ein schöner und ermutigender Erfolg. Im Übrigen haben wir das nur schaffen können, weil wir die Überwachung der ein- und ausgehenden Internetkommunikation dieser Tatverdächtigen über einen langen Zeitraum aufgrund richterlichen Beschlusses durchführen konnten.

Herr Kienzle:

Herr Schürholz, sicher, das ist ein großer Erfolg. Aber haben Sie eine Ahnung oder können Sie präzisieren, wie viel Kriminalität es nach Ihrer Einschätzung im Internet wirklich gibt und wie viel davon Sie aufspüren können?

Herr Schürholz:

Das kann ich seriös nicht. Ich kann davon ausgehen, dass es entsprechend der Zunahme der Internetanschlüsse in der Wirtschaft, im privaten Bereich, in der Wissenschaft, in jedwedem sozialen Bereich einen entsprechenden Prozentsatz krimineller Nutzung oder auch kriminellen Angriffs gegen diese Internetkommunikation gibt. Wie hoch der ist, kann man nur vermuten. Ich denke, das Internet dient inzwischen anstelle anderer Kommunikationsmöglichkeiten und ich schätze die Verbrechensverabredungen im Internet, die jetzt noch in den Augen der Straftäter weitgehend geschützt sind, als hoch ein. Deshalb müssen wir von der Strafverfolgung her, von der Gefahrenabwehr her, dafür sorgen, dass das Entdeckungsrisiko für Straftäter im Internet größer wird.

Herr Kienzle:

Herr Müller-Maguhn, ist das, was jetzt Herr Schürholz gesagt hat – ich gehe davon aus, und das ist ja auch ein spektakulärer Erfolg gewesen mit der Kinderpornographie – ist das ein verschwindend kleiner Teil der Kriminalität im Internet? Gibt es Dinge, die wir gar nicht wissen, oder die Sie vielleicht wissen, aber wir nicht wissen, die Öffentlichkeit nicht weiß? Wie würden Sie das denn einschätzen?

Herr Müller-Maguhn:

Man muss, glaube ich, wirklich die Deliktsform unterscheiden. Kinderpornographie ist weltweit illegal. Das heißt, da haben wir nicht die Probleme, dass die Täter sich in irgendein Land flüchten können und da das machen können. Da stimme ich

ja auch voll mit Herrn Schürholz überein, dass man sagt: Klar, wir müssen hier die Täter ausfindig machen, weil: Eins muss man ja auch bei dieser Auseinandersetzung mit Informationsdelikten – so würde ich das jetzt mal bezeichnen – immer sehen. Es geht hier ja auch nicht darum – und das hat Herr Schürholz auch deutlich gemacht –, dass die Bilder nicht abrufbar sind, sondern es geht darum, dass die Kinder nicht geschändet werden. Also, es geht hier eigentlich nicht um das Internet, sondern um ganz reale physikalische und wirkliche echte Kinder und nicht um irgendwelche bunten Bildchen. Die bunten Bildchen, die führen uns an dieser Stelle zu den Tätern. Und da kann man dann eingreifen und das verhindern. Wenn man so will, ist hier das Netz ja nur ein Medium zur Verabredung von Straftaten oder zur Verkürzung an dem Erfolg von Straftaten oder was auch immer. Es gibt nun aber viele Bereiche, da ist die Lage eben nicht so eindeutig wie bei Kinderpornographie. Da muss ich mir doch die Frage stellen: Macht es irgendeinen Sinn, dass der Staat seine Ressourcen auf Gefechte verlagert, die eben dadurch entstehen, dass in bestimmten Ländern andere kulturelle Vorstellungen, andere historische Abläufe gelaufen sind, dort Dinge eben legal sind? Wenn Deutschland jetzt sozusagen weltweit mit dem Anspruch kommt - wir haben diese Auseinandersetzung ja sehr wohl international erlebt – und sagt: „Also liebe USA. Es kann doch nicht angehen, dass das in eurem Interesse ist, dass Dinge wie Hate Speech über das Internet . . .“ und so fort. Dann kommen natürlich auch andere Länder – die chinesische Regierung allen voran – und sagen: „Ja, wir haben da übrigens auch so ein paar Empfindlichkeiten. Das finden wir nicht toll, dass die in Deutschland solche Sachen verbreiten können.“ Die Angleichung dieser Rechtsverständnisse findet natürlich an verschiedenen Orten, insbesondere im Internet statt. Das ist aber ein sehr langer Prozess. Und in der Zwischenzeit, wo wir sozusagen noch keine globalen einheitlichen Wertvorstellung haben, müssen wir uns erst einmal mit der Realität beschäftigen, die dieses Netz mit sich bringt. Wenn Sie jetzt mich fragen: „Ja, wie sieht es denn aus? Wie viele Verbrechen gibt es da?“ Wir haben auf dieser Tagung schon gehört, dass das Internet im gewissen Sinne dramatische Veränderungen mit sich bringt, wie vergleichsweise die Erfindung des Buchdrucks. Jetzt gibt es noch die Vorstellung der Deklarierung von Eigentumsrechten an Information, also das, was wir hier gehört haben. Microsoft hat hier plastische Beispiele demonstriert, wo CDs kopiert wurden. Bloß, wir wissen alle: Diese CDs sind eigentlich schon überholt. Eigentlich brauchen wir dieses ganze Trägermedium nicht mehr. Das geht über das Internet schneller. Und da ist dann die Frage von Recht und Unrecht eine sehr viel komplexere. Die Durchsetzung von solchen Rechten würde dann sozusagen ein totalitäres Regime erfordern, das dann eben sagt: Diese Information gehört dem und diese Information gehört dem. Die Industrie geht diesen Weg. Das ist das, was unter dem Stichwort Digital-Right-Management-Systeme sozusagen aus zivilrechtlicher Sichtweise gewünscht ist. Aber ob wir als Gesellschaft ein totalitäres Informationsregime wollen, wo der Staat nicht nur dem Bürger Rechte einräumt und andere Dinge verbietet, sondern de facto kontrolliert, wer was tut, das ist die andere Frage. Da bin ich mir natürlich sicher, das wir sagen: Nein, das wollen wir nicht, sondern wir

wollen eine Informationsfreiheit sicherlich unter Achtung der Menschenwürde und unter Achtung der Rechte des andern.

Herr Kienzle:

Eine Zwischenfrage. Was ist bei Ihnen denn ein Verbrechen und was ist bei Ihnen kein Verbrechen?

Herr Müller-Maguhn:

Also über Urheberrechte haben wir ja noch gar nicht geredet. Bei den Rechtsradikalen, da bin ich sicherlich auch der Auffassung, dass es sich um Verbrechen handelt.

Herr Kienzle:

Bei der Kinderpornographie sicher auch, das haben Sie ja auch schon gesagt.

Herr Müller-Maguhn:

Klar, klar. Bloß bei den Rechtsradikalen oder bei politisch extremistischen Äußerungen – da gibt es ja nicht nur rechtsradikale – befürchte ich, werden wir uns gesellschaftlich darauf einstellen müssen, dass diese Informationen für denjenigen, der sie abrufen will, abrufbar sind. Die gesellschaftliche Aufgabe ist es, Zustände zu zeigen, wo das kein Problem ist, wo man damit leben kann, dass eben diese Propaganda als solche entlarvt wird.

Herr Kienzle:

Herr Müller-Maguhn, das ist ein weitgehende Aussage, die Sie gerade gemacht haben und eigentlich auch pessimistisch, wenn Sie sagen: Es ist schlicht und einfach für denjenigen, der es will, immer abrufbar und nicht zu verhindern. Herr Kossel, teilen Sie diese Meinung?

Herr Kossel:

Vom technischen Standpunkt her muss ich diese Meinung teilen. Es gibt sicherlich kein endgültiges absolutes Filterungssystem. Man kann nur Phänomene bekämpfen durch automatische Mechanismen. Man muss dann irgendwo für sich selber entscheiden oder für den Staat entscheiden, wie weit meine Mechanismen gehen dürfen, um einen bestimmten Wirkungsgrad an Filterung zu bekommen. Das derzeitige Filtermodell, wie es Herr Schütte vertritt, halte ich für sehr unzulänglich. Aber wenn man damit weitergeht, dann wird es wirklich schnell sehr schlimm, weil, wenn ich beispielsweise Inhalte oder Neonaziinhalte sicher fernhalten will, dann muss ich anfangen, Inhalte zu filtern. Also ich muss, wenn die Seiten abgerufen werden, im System analysieren: Was steht da drin? Entspricht das bestimmten Stichwörtern? Sind da bestimmte Bilder oder Zeichen drin? Dann filtere ich das. Dann wird es richtig schlimm, denn im nächsten Schritt werden diese Seiten dann verschlüsselt angeboten. Es gibt auch technische Möglich-

keiten, durch ein Zwischensystem die Daten zu entschlüsseln und dann wieder verschlüsselt weiterzusenden.

Herr Kienzle:

Nur eine naive Zwischenfrage: Verschlüsselung bedeutet ja, dass man die Spuren trotzdem verfolgen kann im Internet. Oder bedeutet es, dass die Spuren verwischbar sind? Das ist ein ganz wichtiger Punkt: Verschlüsselung. An dem Punkt würde ich gerne auch mal etwas tiefer gehen. Wie weit ist Verschlüsselung möglich? Wie weit kann ich mir eine Tarnkappe aufsetzen im Internet und durch das Internet gehen, ohne dass ich bemerkt werde? Ist das möglich?

Herr Kossel:

Verschlüsselung ist dann natürlich ein starkes Mittel, wenn die Ermittlungsbeamten darauf angewiesen sind, die Inhalte zu erfassen. Es gibt heute freiverfügbar die notwendigen Programme.

Herr Kienzle:

Noch mal naiv nachgefragt: Ich persönlich kann mein eigenes System so verschlüsseln, dass die Polizei niemals Zugang dazu findet?

Herr Kossel:

Ja, aber das Problem ist immer die Datenmasse. Es mag sein, dass irgendwo bei der NSA ein Rechner steht, der diese Verschlüsselung brechen kann.

Herr Kienzle:

NSA ist die National Security Agency in Amerika.

Herr Kossel:

Nur, dieser Rechner braucht dazu lange. Und es ist ein teueres Verfahren. Das heißt, man kann jetzt nicht anfangen, riesige Datenmengen da reinzuschaufeln. Das ist so ähnlich wie das Beispiel, was Herr Kindler heute gebracht hat mit den beschlagnahmten Kinderpornodateien. Wenn sie natürlich gigabyte-weise solche Daten haben und diese verschlüsselt sind und Sie alles im Prinzip entschlüsseln müssen, dann wird es irgendwann nicht mehr machbar.

Herr Kienzle:

Noch mal eine naive Nachfrage. Vielleicht antwortet Herr Müller-Maguhn darauf. Könnten hochintelligente Kinderpornographen ihr Material so verschlüsseln, dass der Zugang nur möglich ist für einen kleinen Kreis von Verteilern?

Herr Müller-Maguhn:

Ja, aber zunächst einmal: Was die Verschlüsselung nicht löst, ist, wer mit wem kommuniziert. Das heißt das, was Sie als Verbindungsdaten bezeichnen. Und zum andern ist es ja so, dass die Betrachtung dieser Bilder an Bildschirmen ja

nicht verschlüsselt stattfindet. Das heißt, an den Endstellen der Kommunikation haben sie immer noch entschlüsselte Nachrichten. Und zum Dritten haben Sie immer noch richtige, echte Kinder, das heißt: Das ist keine rein virtuelle Angelegenheit, von der wir hier reden, sondern das sind ja auch menschliche Personen, die sich vor Geräten bewegen. Und dort passieren ja die eigentlichen strafbaren Handlungen. Alles andere sind sozusagen nur Mittel, die zur Vernetzung, vielleicht zur Verabredung, zur Organisation dieser Straftaten benutzt werden. Dort haben sie selbstverständlich alle Möglichkeiten der kriminalpolizeilichen Arbeit. Verschlüsselung ist ein Mittel, um nicht nur die Datenwege, sondern auch die gelagerten Daten relativ abzusichern. Relativ heißt aber natürlich auch – Herr Schily hat es auch erwähnt – dass es ja das Bundesamt für Sicherheit und Informationstechnik gibt, das auch einen Aufgabenbereich „Kryptanalyse“ hat. Wie gesagt, ich glaube, soweit müssen Sie gar nicht gehen. Bei vielen Straftaten, von denen wir hier reden, handelt es sich nicht um elektronische Straftaten im eigentlichen Sinne, sondern sie basieren auf vermeintlichen Urheberrechtsverletzungen.

Herr Kienzle

Sie müssen dann auch praktisch den Nutzer am Bildschirm erwischen.

Herr Müller-Maguhn:

Das ist nicht in allen Bereichen die notwendige Konsequenz – und ob sie dazu die gesetzlichen Grundlagen, geschweige die Mittel zur Umsetzung zur Verfügung haben, ist die nächste Frage. In vielen Bereichen spielt sich die Kriminalität ja nicht auf dem Bildschirm, sondern davor ab.

Herr Kienzle:

Habe ich das richtig gehört? Wenn er sagt: In diesen verschlüsselten Prozess kann ich nicht eindringen, bleibt Ihnen doch eigentlich jetzt logisch gesehen nur die Möglichkeit, dort, wo tatsächlich real auf dem Bildschirm geguckt wird, zuzugreifen.

Herr Müller-Maguhn:

Nein, hier müssen wir differenzieren. Bei der Diskussion um extremistische Internetseiten geht es ja um medienrechtliche Fragen, also der Frage wer die Verantwortung für die Verfügbarkeit derartiger Inhalte hat – dazu müsste Herr Schürholz vielleicht etwas sagen.

Die Kernfrage ist hier, welche Verpflichtungen Internet-Service-Provider, also Zugangsvermittler haben, und nicht die mögliche Strafbarkeit von Handlungen der Nutzer.

Bei der Verschlüsselung geht es im Wesentlichen um den Punkt-zu-Punkt-Verkehr. Wenn ich also in elektronischer Form verschlüsselt mit einem spezifischen Gesprächspartner in Kommunikation stehe. Aber bei der Medienrechtsdiskussion geht es definitiv nicht um verschlüsselte Angebote, weil hier ja Inhalte eine Öf-

fentlichkeitswirkung erzielen sollen; diese Angebote sind ja vom Charakter her frei zugänglich.

Herr Kienzle:

Herr Schürholz, kann Verschlüsselung verboten werden?

Herr Schürholz:

Wenn der Gesetzgeber dieses machen würde, könnte er theoretisch so vorgehen, dass er Verschlüsselungsverfahren nur zulässt im Genehmigungswege und bei Hinterlegung eines Nachschlüssels für den Fall notwendiger Ermittlungen.

Herr Kienzle:

Können Sie sagen, in welchen Staaten das probiert worden ist?

Herr Schürholz:

Die USA und Frankreich wollten diesen Weg gehen, aber es funktioniert deshalb nicht, weil es ein weltweites Regelungsproblem wäre. Und infolgedessen muss man einen anderen Weg gehen, damit auch kryptierte Kommunikation für die Ermittlungen kein Hindernis ist. Man müsste Ausgleichsmaßnahmen und Umwegsmaßnahmen ergreifen. Das heißt, vor oder nach der Kryptierung auf die entsprechende Kommunikation zugreifen. Dieses ist der praktikable Weg. Herr Müller-Maguhn hat es angedeutet. Meines Erachtens hätte dieser Weg schon längst begangen werden müssen. Es war sicherheitspolitisch nicht zielführend, dass die Bundesregierung im Jahr 1999 so genannte Grundsätze der Kryptopolitik beschlossen hat, in denen sie gesagt hat: Das ist ein so wichtiger Vorgang für die weitere Nutzung des Internets und für die wirtschaftliche Entwicklung, insbesondere im Bereich E-Commerce, dass sich hier Verschlüsselungsverfahren möglichst gut entwickeln und verbreiten können. Dabei hat die Bundesregierung Abstand genommen von Vorkehrungen, wie man trotz Verschlüsselungstechnik die notwendige und justiziell angeordnete Überwachung von Täterkommunikation im Internet sicherstellen kann.

Herr Kienzle:

Was würden Sie sich denn wünschen?

Herr Schürholz:

Ich wünsche mir technische, organisatorische und rechtliche Grundlagen, um Verschlüsselung zu überwinden. Davon erwarte ich mir eine brauchbare und umsetzbare Lösung.

Herr Kienzle:

Haben Sie denn reale Erfahrungen mit Verschlüsselung? Und ist es Ihnen gelungen, diese zu durchbrechen?

Herr Schürholz:

Wir haben reale Erfahrungen mit der Tatsache, dass wir auf verschlüsselte Täterkommunikation treffen, die wir nicht überwinden können. Diese reale Erfahrung veranlasst uns zu sagen: Wir brauchen hier den Zugriff auf kryptierte Täterkommunikation, auch wenn es nur auf Umwegen, auf technischen Umwegen geht.

Herr Kienzle:

Herr Müller-Maguhn. Ist dieser Wunsch verständlich? Und würden Sie ihn auch akzeptieren?

Herr Müller-Maguhn:

Verständlich ist er sicherlich. Aber er betrachtet leider die Sachlage nicht in dem gebotenen Umfang, weil ein Kryptoverbot für Produkte, die keinen staatlichen Nachschlüssel erhalten, ja die Annahme voraussetzt, dass sich Kriminelle an Gesetze halten. Und das brauche ich, glaube ich, nicht weiter ausführen. Im Gegenteil würde das die ehrbaren Bürger treffen, die dann, weil sie sich an Gesetze halten, nur Verschlüsselung einsetzen, die einen staatlichen Nachschlüssel enthält. Und dieser birgt ja nicht nur die Chancen, wenn der ehrliche Bürger dann mal zu einem unehrlichen wird oder doch zu einem Straftäter, auf seine Kommunikation zuzugreifen, sondern auch ein enormes Missbrauchspotenzial nicht durch kriminalpolizeiliche Arbeit, sondern durch die Tatsache, dass hier technisch dann Angriffspunkte erstellt werden und zentrale Entschlüsselungszentralen zentrale Begehrlichkeiten wecken und sozusagen organisierter krimineller Zugriff geradezu prädestiniert ist in diesen Bereichen. Deswegen hat die Bundesregierung eben auch den, wie ich meine, sehr weisen Entschluss gefasst und gesagt: Mit so einem Unsinn wollen wir uns nicht weiter beschäftigen. Wir wollen jetzt mal einen Punkt setzen und uns darauf konzentrieren, was technisch sinnvoll und machbar ist. Andere Länder haben das auch getan.

Herr Kienzle:

Was ist denn sinnvoll? Und was ist machbar?

Herr Müller-Maguhn:

Wie gesagt: Kriminalpolizeiliche Arbeit, befürchte ich, war immer mühsam und wird es immer sein, weil Täter nun mal nicht offen herumlaufen und ihre Straftaten propagieren – gut, einige tun auch das. Aber das ist wohl eher die Minderheit –, sondern weil Kriminalität normalerweise im Verborgenen stattfindet und man da in irgendeiner Form darauf zugreifen muss. Bloß, ich denke, das Internet – bei aller Abscheu, die wir vielleicht für diese Straftaten hier empfinden – bietet auch eine Chance, dass bestimmte gesellschaftliche Zustände und Probleme überhaupt erst richtig sichtbar werden.

Herr Kienzle:

Können Sie das konkreter machen?

Herr Müller-Maguhn:

Ganz konkret: Wenn wir von Kinderpornographie reden: Für mich ist da nicht das Internet ein Problem, sondern das Problem sind erwachsene Menschen, die sich hier an Kindern vergehen. Offenbar gibt es da ein Missverhältnis in der Gesellschaft, dass hier so etwas überhaupt passiert. Eigentlich meine ich, ist das Internet ein wunderbares Medium, um solche gesellschaftlichen Missstände diskutierbar zu machen, erfahrbar zu machen und auch darüber zu reden, wie man denn mit solchen Tätern umgeht. Hier geht es auch konkret um die Frage: Wie verhält man sich als Bürger, wenn man vielleicht zufällig im Internet so etwas sieht? Ich glaube nicht, dass sie allzu viele Polizeistreifen brauchen.

Herr Kienzle:

Das ist ein interessanter Ansatzpunkt. Sie fordern nicht nur die Polizei, sondern die Gesellschaft und die Einzelnen auf, sich zu beteiligen.

Herr Müller-Maguhn:

Auf jeden Fall.

Herr Kienzle:

Herr Kossel. Ist das ein gangbarer Weg?

Herr Kossel:

Das ist sicherlich ein wichtiger und sehr gangbarer Weg. Ich koordiniere jetzt schon seit einigen Jahren bei uns dieses Netz gegen Kinderpornographie. Das wurde damals ins Leben gerufen, als uns auffiel, dass immer mehr Leser klagten, sie fänden tatsächlich zufällig Kinderpornographie im Internet, wagten es aber nicht, damit zur Polizei zu gehen, weil es in dieser Zeit einige Fälle gab, wo gegen Melder dann direkt ermittelt wurde. Denn sie waren ja im Besitz von Kinderpornographie, was strafbar ist. Wir haben daraufhin eine Meldestelle eingerichtet, haben die Meldungen entgegengenommen, anonymisiert und dann mit der Staatsanwaltschaft in Hannover zusammengearbeitet und dort diese Meldungen abgeliefert. Es war erschreckend, wie viele Meldungen kamen. Das waren 200 bis 300 Meldungen im Monat, die aus dem ganzen Bundesgebiet eingingen. Schließlich wurde es dann immer schwieriger, eben für die Staatsanwaltschaft in Hannover, da man nicht genau entscheiden konnte, war der Fund jetzt in Bayern, müssen wir es dahin weiterleiten, das zu koordinieren. Gott sei Dank ist das LKA in Nordrhein-Westfalen auf uns zugekommen und hat gesagt: Wir organisieren eine Umfrage bei allen LKÄ und geben euch ein Statement, dass künftig gegen Erstfinder, die im Internet auf Kinderpornographie stoßen und das melden, nicht ermittelt wird. Das gab uns schließlich die Möglichkeit, diese Meldestelle einzustellen.

Wir haben stattdessen heute eine Seite mit Kontaktadressen der 16 LKÄ. Und da muss ich sagen, ist die Zusammenarbeit sehr schlecht. Diese Adressen ändern sich. Plötzlich kommen die E-Mails wieder zurück. Wir werden darüber natürlich nicht informiert. Ich frage nach. Ich hab schon in mehreren Fällen E-Mail-Adressen genannt bekommen – von LKÄ, die zu dem Zeitpunkt, als ich sie genannt bekommen habe, nicht erreichbar waren. Ich habe da teilweise den Eindruck, man möchte sich gar nicht mit dieser Meldungsflut auseinander setzen. Dabei wäre das doch wirklich ein Mittel, um den aufmerksamen, vernünftigen, mündigen Bürger mit in die eigene Arbeit einzubeziehen.

Herr Kienzle:

Herr Schütte, das ist zumindest verwunderlich, was ich eben gehört habe. Da ist ein Angebot der Zusammenarbeit. Und es wird – ich sag jetzt nicht von Ihrer Seite persönlich –, sondern von Seiten der Polizei offensichtlich nicht ernst genommen.

Herr Schütte:

Auf die Beteiligung der Gesellschaft haben wir ja auch zunächst gesetzt. Ich denke, die Provider sind auch Teil der Gesellschaft. Und wir haben seit 1997 mit den Providern gesprochen. Wir haben zahlreiche Veranstaltungen gehabt. Herr Büssow als Regierungspräsident in Düsseldorf hat des öfteren Provider eingeladen und sie dringend gebeten, rechtsextreme Seiten zu sperren. Die Provider waren dazu nicht bereit. Deswegen ist es im Jahre 2002 zu den Sperrverfügungen gekommen. Wir würden es natürlich als wünschenswert ansehen, wenn die Provider – diesmal haben wir staatlichen Druck ausgeübt – freiwillig bereit wären, gegen solche Inhalte vorzugehen.

Herr Kienzle:

Polizisten sozusagen in Zivil. Herr Schürholz.

Herr Schürholz:

Wie im realen Raum sind wir auch im virtuellen Raum darauf angewiesen, dass Bürger etwas wahrnehmen und, wenn es etwas Kriminelles, Leben, Gesundheit, seelische Unversehrtheit Bedrohendes ist, dieses dann auch der Polizei oder anderen Stellen mitteilen, die schnell und wirksam eingreifen können. Das wollen wir mit aller Kraft fördern. Wo es Schwierigkeiten etwa in der Adressierung und in der Zusammenarbeit gibt, wären wir wirklich dankbar, wenn uns das auch auf Leitungsebene bekannt gemacht würde. Ich denke, wenn es da Kommunikationsprobleme gibt, wird jeder von uns für schnelle Abhilfe sorgen.

Herr Kienzle:

So viel Gemeinsamkeit hatte ich ja gar nicht erwartet. Das ist ja schon ein wichtiger Schritt, finde ich. Aber ich werde zum Schluss noch ein ganz wichtiges Thema ansprechen. Das ist der Terrorismus. Wir haben ja den realen Terrorismus „Nine Eleven“ erlebt. Dieser reale Terrorismus hat nach Schätzungen von Wirt-

schaftsfachleuten einen Schaden von ca. 1.000.000.000.000 Dollar verursacht in Amerika, unter anderem mit in die Rezession gebombt, wenn man es so ausdrücken darf. Ist der Cyberterrorismus vergleichbar mit dem, was der reale Terrorismus in den letzten Jahren erreicht hat, Herr Müller-Maguhn? Kann man darüber überhaupt etwas sagen?

Herr Müller-Maguhn:

Zunächst mal: Cyberterrorismus ist ein Begriff, der ein bisschen fragwürdig ist. Immer wenn im Internet Systeme angegriffen werden, um einmal das andere Extrem zu zeigen, dann sehen Sie in den diversen Zeitschriften die armen Systeme, die angegriffen werden. Dann sehen Sie eine Wolke. Da steht Internet. Und dann sind da in der Regel so genannte Hacker, die es gewesen sein sollen. Auch hier auf dieser Tagung habe ich den Begriff „Hacker" sehr undifferenziert vorgefunden. Eigentlich muss man sagen: Information Warfare. Das heißt, die Beschäftigung normaler Armeestrukturen mit Methoden des Angriffs der Zersetzung, der Manipulation von IT-Strukturen ist quasi in jedem Land auf diesem Planeten vorhanden. Mittlerweile gehört das zum Grundsatzverhalten von militärischen Strukturen, auch und gerade bei Ländern, die sonst nur sehr kleine Armeen aufgrund ihrer beschränkten Budgets haben, weil die Information Warfare eben im Vergleich zu konventionellen Waffen fast nichts kostet. Das heißt, vieles wird da in den letzten Jahren auch ausprobiert von Regierungsstellen allerdings, nicht von Hackern, um eben mal auszuprobieren, wie man Systeme sozusagen effektivst möglich angreift.

Herr Kienzle:

Das Militär als Hacker. Das ist ja auch eine interessante Variante.

Herr Müller-Maguhn:

Die Hacker sind halt das Standardfeindbild. Man kann dann immer sagen: Die waren es und sich da hinter wunderbar verstecken. Die Angriffe unter falscher Flagge, wie es im militärischen Sprachgebrauch heißt, sind eine ganz normale Methode. Und im Internet geht das natürlich sehr viel einfacher. Wenn ich den Begriff Cyberterrorismus höre, klingt das für mich in erster Linie und in den meisten Kontexten lediglich wie eine Budgetrechtfertigungsmaßnahme für bestimmte neue Sicherheitsinstitutionen, die mit sehr fragwürdigen Argumenten sehr fragwürdige Dinge tun, nämlich beispielsweise eine vollständige Überwachung des Internetverkehrs zu fordern, um die so genannten Terroristen, die man möglicherweise auch selbst ausgebildet hat, dann sozusagen zu detektieren. Insofern sehe ich das ein bisschen schwierig. Auf der anderen Seite gibt es natürlich Angriffsmethoden auf diese Infrastrukturkomponente, die in allen gesellschaftlichen Bereichen, also wirtschaftlich wie auch kulturell und soziales Leben, heute auf IuK-Strukturen basiert. Und entsprechend gibt es natürlich auch eine höhere Anfälligkeit der Gesellschaft. In Deutschland haben wir ein sehr gesundes Verhältnis der Trennung zwischen kritischen Infrastrukturen und so etwas wie dem Internet. Aber die Befürchtung steht natürlich im Raum aufgrund der Kostensenkungsdrü-

cke, die da entstehen. Man sagt ja: Diese und jene Standleitung. Die ersetzen wir jetzt mal durch diese IP Internet DSL-irgendwas-Verbindung. Und dann ist man ganz schnell in Teufelsküche. Insofern, ist da ein reales Gefahrenpotenzial. Noch bewegt der gesunde Menschenverstand in dieser Republik auch einige Dinge zum Positiven. Aber ich denke: Vor allem muss man sich mal differenziert auch bei den Ermittlern damit beschäftigen, was da so passiert, weil viele Angriffe möglicherweise auch unmittelbar von denen kommen, denen sie nützen. Und das sind dann die Vertreter der so genannten Sicherheitsindustrie. Auch dort, denke ich, weiß der eine oder andere von ihnen, dass man die Spreu vom Weizen mal trennen muss.

Herr Kienzle:

Ich fand das sehr gut, dass Sie mal den Begriff Cyberterrorismus etwas präzisiert haben. Meine Frage an Sie, Herr Kossel.

Herr Kossel:

Der reale Terrorismus ist ja eine Riesengefahr, wie wir an den wirtschaftlichen Geschichten gesehen haben. Und ich glaube nicht so sehr an die Verschwörungstheorien. Der Cyberterrorismus ist eine Gefahr, die ähnlich werden kann oder ist wie der reale Terrorismus, der islamistische Terrorismus. Und kommen wir – und das ist ein ganz wichtiger Punkt – bei den Kommunikationswegen, die diese islamistischen Terroristen heute verfolgen, überhaupt an Quellen heran? Es stellt sich ja heraus, dass, nachdem Binalshibh und Cheikh Mohamed per Handy geschnappt worden sind – das hat ja am Dienstag Herr Glotz formuliert – man zu mittelalterlichen Methoden zurückkehrt, nämlich zu den schlichten Boten. Und es gibt im Orient ja seit langer Zeit die Überweisungstechnik der Hauala, eine Banktechnik, die keine Spuren hinterlässt: Wer nicht zahlt, wird umgelegt. Das ist sehr erfolgreich, ganz offensichtlich. Das heißt: Hat unsere High-Tech-Welt überhaupt die Fähigkeit, diese neuen Strukturen oder diese alten Strukturen zu erkennen und in sie einzudringen? Das finde ich ja im Zusammenhang mit dem Terrorismus eine ganz wichtige Frage: Lassen die das Internet einfach links liegen oder rechts liegen und benutzten es nicht? Saddam Hussein. Wie kann es passieren, dass ein Staat wie Amerika, der solche High-Tech-Geräte hat, einen Mann nicht findet, der offensichtlich mit 1.000 oder mehr Leuten unterwegs ist und kommunizieren muss. Das heißt, diese Frage: Inwieweit wird das Internet genutzt für Terrorismus von Terroristen, um sich zu informieren? Gibt es da überhaupt Vorstellungen? Gibt es keine? Wird es genutzt? Das ist eine ganz wichtige Frage. Gut. Also diese Frage, inwieweit das Internet von Terroristen genutzt wird, sollte man sicherlich eher dann an die Spezialisten hier stellen. Das Thema Cyberterrorismus an sich halte ich auch nicht so für bedeutend oder zumindest für stark übertrieben und natürlich auch durch Hollywoodfilme immer gut illustriert: Der High-Tech-Spezialist, der eine Flughafensteuerung lahm legt, Flugsicherung lahm legt usw. Ich denke, Terrorismus entwickelt sich im Moment in eine ganz andere Richtung. Das ist der Selbstmordattentäter, der mit seiner Bombe vorfährt und die zündet.

Herr Kienzle:

Die falsche Methode.

Herr Kossel:

Ja. Das sind einfache Kommunikationsmittel, die eben gerade diese High-Tech-Gesellschaft umgehen. Und das sind ganz einfache brutale Methoden, die in dieser High-Tech-Gesellschaft viel tiefer einschlagen als irgendwelche Hackerangriffe. Terrorismus hat heute ganz andere Ziele und ganz andere Methoden. Vielleicht geht irgendwo mal an einem zentralen Internetknoten, über den die Kommunikation eines Kernkraftwerks läuft, eine Bombe hoch und die Katastrophe wirkt dann indirekt. So etwas könnte ich mir noch vorstellen. Aber dieser Begriff „Cyberterrorismus“, den halte ich etwas an den Haaren herbeigezogen.

Herr Kienzle:

Herr Schürholz, Sie als Praktiker. Wie sehen Sie das?

Herr Schürholz:

Ich denke, es gibt viele Facetten und viele Motive des Terrorismus in vielen Regionen. Das ist sehr schwer auf einen Nenner zu bringen. Ich würde es auf keinen Fall ausschließen, dass sich terroristische Aktionen auch und gerade symbolhaft gegen kritische Infrastrukturen der Kommunikation richten werden. Deshalb muss auch in diesem Bereich Gefahrenvorsorge betrieben werden.

Herr Kienzle:

Wie soll die aussehen?

Herr Schürholz:

Das hat gestern der Vertreter des BSI angedeutet. Das heißt, man muss sich im Wege möglicher Szenarien überlegen, was da geschehen könnte. Mit Hilfe von Technikern und denjenigen, die den unmittelbaren Zugriff auf diese Bereiche haben, also denjenigen, die die Verantwortlichen der kritischen Infrastrukturen sind, IT-Sicherheit, und zwar in einem sehr systematischen und umfassenden Sinn betreiben. Da möchte ich noch mal bei dieser Gelegenheit ein bescheideneres Angriffsszenario, was gestern auch Gegenstand hier der Erörterungen war, aufgreifen. Die Angriffe durch die Würmer, die wir in der letzten Zeit erlebt haben. Ich wundere mich, warum nicht auch von Providerseite mal die Möglichkeit ergriffen worden ist, dieses schon auf der Ebene der Knoten, die bei den Providern liegen, mit intelligenten Möglichkeiten der Abwehr

a) zu finden und dann

b) aufzuhalten.

Warum muss das denn auf die Ebene der Nutzer überhaupt erst kommen . Warum kann das nicht schon auf der Ebene der Provider und der Knoten entdeckt und aufgehalten werden.

Herr Kienzle:

Herr Schürholz. Jetzt sind Sie mir natürlich sehr geschickt ausgewichen. Ich habe ja eine andere Frage gestellt. Wie bekämpfen wir diese Formen von Terrorismus? Gibt es da bei Ihnen Vorstellungen? Wir haben ja gehört: Cyberterrorismus ist nicht so sehr die Gefahr, sondern es gibt eben Kommunikationswege, die völlig anders verlaufen. Und die Rasterfahndung – das haben wir ja gemerkt, oder das wissen wir heute – hätte im Fall der islamistischen Terroristen uns relativ wenig gebracht, weil sie still und ruhig gelebt haben bis zu dem Augenblick, wo sie zugeschlagen haben. Gibt es denn da ein neues Nachdenken auf Seiten der Polizei, da weiterzukommen? Das Eindringen in solche Zirkel ist ja fast unmöglich.

Herr Schürholz:

Ich denke, Polizei und Justiz in Bund und Ländern sind da gar nicht ohne Erfolge in der Zwischenzeit. Und zwar, wie Sie auch schon vermutet haben, mit ganz gewöhnlichen kriminalistischen Ermittlungen gegen mögliche Gefährder. Da sind wir auch längst weg von der Vorstellung eines zentral-organisierten und -strukturierten Terrorismus. Gerade im Bereich des islamistischen Terrorismus gehen wir von einer eher lockeren Vernetzung relativ autonom handelnder regionaler Strukturen aus, die aber durchaus miteinander kommunizieren. Und gegen diese Strukturen haben wir schon eine ganze Menge von Ermittlungserfolgen erzielt, zum Beispiel bei ihrer Logistikkriminalität. Überall dort, wo sie sichtbar werden müssen, um nämlich ihre terroristischen Planungen und Vorkehrungen überhaupt finanzieren zu können, durch Beschaffungskriminalität, die sie begehen. In diesen Bereichen, denke ich, waren wir offensiv und durchaus mit herkömmlichen Mitteln erfolgreich.

Herr Kienzle:

Herr Schütte, angesichts der fortgeschrittenen Zeit ein Schlusswort von Ihnen. Haben Sie heute etwas von der anderen Seite gelernt? Und wenn ja: was?

Herr Schütte:

Ich muss ehrlich sagen, ich kenne die Argumente der anderen Seite schon seit längerem.

Herr Kienzle:

Das heißt, Sie haben nicht viel gelernt.

Herr Schütte:

Nein, gelernt habe ich, sage ich mal, die klare Sprache, die Herr Müller-Maguhn heute gesprochen hat, als er sagte: Wenn es eine Filterung denn gäbe oder eine Speicherung von Internetangeboten, müsse diese sozusagen vor dem Endgerät stattfinden. Das, finde ich, ist eine Aussage in einer Klarheit, die er so bisher nicht getan hat. Das ist wirklich, sag ich mal, der grundlegende Meinungsunterschied,

den wir wahrscheinlich miteinander haben. Ich sage oder wir sagen: Es gibt eine staatliche Schutzpflicht. Der Staat darf sich hier nicht heraushalten. Entsprechend versuchen wir auch zu handeln, so schwer es auch ist.

Herr Kienzle:

Herr Kossel, haben Sie denn etwas von der anderen Seite gelernt?

Herr Kossel:

Ja gut, ich habe die ganzen Tage recht viele interessante Sachen gehört. Ich habe natürlich ein bisschen Verständnis dafür gewonnen, wo die Schwierigkeiten und die Probleme der Ermittler liegen. Dass ihre Ziele richtig sind, darüber muss man hier nicht diskutieren.

Herr Kienzle:

Und Sie wollen ihnen auch helfen?

Herr Kossel:

Ich möchte ihnen gerne helfen. Ich möchte aber nicht, dass jenseits jeglicher Verhältnismäßigkeit spezielle Gesetze, spezielle Rechtsräume für das Internet geschaffen werden, weil man Angst hat, dass man sonst quasi in die Online-Anarchie verfällt. Dieser Gefahr kann man, denke ich, mit einer gewissen Verhältnismäßigkeit und auch mit bestehenden Normen, die man umsetzt, begegnen.

Herr Kienzle:

Also, ein bisschen Anarchie soll bleiben?

Herr Kossel:

Ein bisschen Anarchie darf ruhig bleiben, ja.

Herr Kienzle:

Herr Müller-Maguhn. Ein Schlusswort von Ihnen.

Herr Müller-Maguhn:

Ich denke, in der Tat ist eines klar geworden, nämlich dass sich die polizeiliche Ermittlungsarbeit zum Teil dahingehend neu strukturieren muss, dass die Teilhabe an bestehenden Kommunikationsprozessen verbessert werden muss, auch wenn man vielleicht normalerweise gewohnt ist, Kommunikationsprozesse, die man betreibt, auch zu steuern. Das wird im Internet vielleicht nicht immer möglich sein. Aber es ist ja deutlich geworden, dass es teilweise an Ansprechpartnern fehlt, um Missstände der ordnungsgemäßen polizeilichen Bearbeitung zuzuführen. Das hat sicherlich auch damit etwas zu tun, dass man sich vielleicht hier und da noch ein bisschen mehr mit den technischen Grundlagen beschäftigen muss. Ich darf bei der Gelegenheit auch darauf hinweisen, dass es natürlich auch hilfreich wäre, wenn die Polizei bei dem eigenen Einsatz dieser elektro-

nischen Mittel mal ein bisschen gucken würde, wessen Infrastruktur sie sich da bedient. Es gibt da dieses Beispiel einer ausländischen Firma, die Soft- und Hardwarekomponenten für gesetzmäßiges Abhören liefert. Sie waren in Amerika in der Presse, weil da leider eine andere Regierung auch immer mithört. In Holland waren sie in der Presse. Auch in Deutschland waren sie in der Presse. Und jetzt höre ich gerade – ich habe mich während der Tagung ein bisschen umgehört – dass beispielsweise Berlin und andere Bundesländer diese Software trotzdem einsetzen, obwohl man eigentlich meinen müsste, bei ihnen im Raum doch der Wissensstand vorhanden sein muss, dass sie damit ja gerade ihren so genannten islamistischen Terroristen nebenbei noch die Informationen liefern. Ich denke, da muss noch ein bisschen was passieren. Der Informationsaustausch zwischen den vielen Institutionen, die sich hier in diesem Rahmen versammelt haben, muss noch ein bisschen verbessert werden. Auch dazu gibt Ihnen dieses Internet übrigens hervorragende Möglichkeiten für Ihre Arbeit zur Hand. Und dabei wünsche ich Ihnen dann viel Erfolg.

Herr Kienzle:

Meine Damen und Herren, das war ein sehr persönliches Schlusswort. Ich bedanke mich für die spannende Diskussion. Ich hoffe, dass alle etwas gelernt haben. Ich wünsche, dass ein Teil dessen, was von der einen Seite kam, vielleicht auf der anderen Seite wirklich ankommt und ernst genommen wird. Dann wäre es ein sehr produktives Gespräch gewesen.

Prof. Dr. Jürgen Stock, Abteilungspräsident im BKA, war ein stets aufmerksamer Tagungsleiter

Verabschiedung

Ulrich Kersten

Herr Kienzle, herzlichen Dank für die Führung und Leitung, dieses, wie wir das traditionell nennen, Streitgesprächs! Ich denke, es war in anständigem Rahmen ein Streitgespräch. Viele interessante unterschiedliche Auffassungen sind deutlich geworden. Herzlichen Dank dafür auch den Teilnehmern an dieser Podiumsdiskussion!

Meine Damen und Herren, liebe Kolleginnen und Kollegen, eine Arbeitstagung geht zu Ende, die uns eine Fülle von Informationen gebracht hat, die in Teilen – für mich jedenfalls – auch sehr spannend war, die vor allen Dingen sehr deutlich Probleme, Defizite, Meinungsunterschiede angesprochen hat.

Wir sind auf dem Weg oder vielleicht schon angekommen mit Aussichten in der modernen Informationsgesellschaft, die niemand so recht definieren kann. Dass dieses nicht nur Vorteile für das Wirtschaftsleben, für Produktionsprozesse, für Administrationsprozesse und auch in unserem privaten Bereich große Veränderungen und Auswirkungen hat, ist deutlich geworden. Genauso ist deutlich geworden, dass mit dieser „schönen neuen Welt" auch Schattenseiten verbunden sind, Schattenseiten, die uns als Polizei, als Strafverfolgungsbehörden, nicht ruhig sein lassen können.

Wir haben gerade jetzt hier auch zum Schluss in der Podiumsdiskussion gehört, dass durch diese Veränderungen auch Anforderungen an Veränderungen in unserem Denken erforderlich sind.

Was für mich in den drei Tagen immer wieder deutlich wurde, ist, dass Meinungsunterschiede zum Teil in den klassischen Denkmustern vorgetragen und abgewickelt werden. Diese klassischen Denkmuster, die sicherlich im Kern etwas haben, was unverändert besteht, nämlich Freiheitsrechte, aber auch der Anspruch des Bürgers auf Sicherheit. Aber ich habe Zweifel, ob wir wirklich schon so weit sind, dass wir uns auf die neuen Bedingungen auch mit neuen Argumenten einstellen. Das sage ich für alle Beteiligten. Insofern, Herr Müller-Maguhn, greife ich Ihr Schlusswort auf. Ich halte es für dringend erforderlich, dass alle Beteiligten staatlicherseits, aus der Wirtschaft, aus dem Bereich des Datenschutzes, auch der Presse, sehr viel mehr miteinander kommunizieren und vorbehaltlos ihre Argumente und Gesichtspunkte austauschen und zu hoffentlich für alle tragbaren Lösungen kommen. Dass dies ein schwieriger Prozess ist und wir in vielen Dingen noch in Köpfe hineinmüssen, das scheint mir auf der Hand zu liegen.

Die Strafverfolgungsbehörden, die Polizei vertreten den Standpunkt: Das, was sich in der so genannten klassischen Kriminalität abspielt, kann nicht ohne Sanktion, ohne Verfolgung bleiben, nur weil es sich in die virtuelle Welt begibt. Dass wir vor neue Herausforderungen gestellt sind, wenn wir Kriminalität in dieser vir-

tuellen Welt aufdecken, definieren und verfolgen wollen – auch das ist deutlich geworden – ist unbestritten. Und dabei muss man auch darüber nachdenken, ob Polizei und Strafverfolgungsbehörden das dafür nötige Instrumentarium haben. Soweit es nicht vorhanden ist oder nicht geeignet ist, weil die neuen Bedingungen zu diesen vorhandenen rechtlichen Rahmenbedingungen und Ausformungen dieses Rahmens nicht passen, dann denke ich, muss man darüber nachdenken und muss es legitim sein zu fordern, dass die entsprechenden Anpassungen erfolgen.

Nur damit hier kein Missverständnis im Raum bleibt. Herr Kienzle, Sie haben sehr pointiert danach gefragt, was die Forderung aus dem Bereich der Strafverfolgung, der Polizei anbelangt, dass die Provider verpflichtet werden sollen, gesetzlich verpflichtet werden sollen, Verbindungsdaten zu erheben und für eine bestimmte Zeit zu speichern für Zwecke der Strafverfolgung – wie wir gehört haben ein strittiges Thema. Dieses ist von der Bundesregierung aufgenommen. Das hat der Bundesminister des Innern hier vorgestern in seiner Eröffnungsansprache erklärt. Der Bundesminister des Innern hat auch gesagt, dass er die polizeiliche Forderung für nachvollziehbar hält. Aber er hat darauf hingewiesen, dass hier eine Interessenabwägung stattfinden muss mit den Gesichtspunkten des Datenschutzes und auch der Wirtschaft, weil letztendlich hier auch finanzielle Interessen eine Rolle spielen. Von diesem Abwägungsprozess hat er gesprochen und hat darauf hingewiesen. Dieser Prozess ist noch nicht abgeschlossen.

Rahmenbedingungen, rechtliche Rahmenbedingungen. Ich habe jetzt eine genannt. Für mich ein ganz wichtiger Punkt. Auch dieses ist während dieser Tagung angesprochen worden. Eine Kriminalität, die sich aufgrund der technischen Gegebenheiten nicht nur national, sondern grenzüberschreitend im internationalen globalen Raum abspielt, ist ohne internationale Zusammenarbeit der Strafverfolgungsbehörden nicht denkbar. Hier sind die Voraussetzungen zum Teil noch ungenügend. Es ist angesprochen worden, dass es unterschiedliche rechtliche Standards, auch unterschiedliche rechtliche Grundauffassungen gibt. Freiheit der Meinungen ist angesprochen worden. In den USA wird das anders interpretiert als zum Beispiel bei uns. Wir sind immer noch auf Rechtshilfe angewiesen. Die Rechtshilfe ist auf diese Art von Kriminalität teilweise noch nicht in ihren Voraussetzungen und Bedingungen eingestellt. Daran muss gearbeitet werden. Es ist die Cybercrime-Konvention von 2001 erwähnt worden. Ich halte das für den richtigen Weg. Ich bin überzeugt, es ist nicht der letzte Meilenstein auf diesem Wege.

Wir brauchen im Übrigen eine genügende Aus- und Fortbildung. Wir brauchen Spezialistenwissen, wenn wir einigermaßen mit Erfolg gegen Kriminalität, die sich in dieser neuen virtuellen Welt abspielt, bestehen wollen. Bei einigen Vorträgen ist mir aufgefallen – vielleicht liegt es an meinem Alter –, dass auch in einer neuen Sprache geredet wird. Sowohl von der Diktion, als auch von den Inhalten her. Ich bin nicht mit dem Internet geboren worden. Als ich geboren wurde, gab es schlicht Telefonverkehr, allerdings mit menschlicher Vermittlung. So ändern sich die Zeiten. So ändert sich Sprache. So ändern sich Begriffe.

Ich denke, es ist deutlich geworden, dass dies bedeutet: Wir müssen unsere Beamten, und zwar nicht nur in der Polizei, sondern auch in der Justiz, und alle anderen, die auch an diesem Feld arbeiten, in den Stand versetzen, nachzuvollziehen, nachvollziehen zu können, was sich eigentlich abspielt. Dies ist eine Aufgabe von Dauer, schon deswegen, weil sich ständig etwas Neues ergibt und dann auch in der Ausbildung ständig nachgebessert werden muss. Dies ist eine Aufgabe, die Geld kostet. Dies ist eine Aufgabe, die ohne gleichzeitig stattfindende technische Ausstattung für die Polizeibehörden, für die Staatsanwaltschaften, kaum zu bewältigen sein wird. Der Bundesminister des Innern hat hier jedenfalls für den Bund die Aussage getroffen, dass hier die Priorität auch unter haushaltsrechtlichen Gesichtspunkten in der Bundesregierung gesehen wird.

Ganz wichtig scheint mir zu sein, dass mehr als bisher dem Gesichtspunkt der Vorbeugung, der Verhinderung Rechnung getragen wird. Dabei komme ich auf das Stichwort „IT-Sicherheit“. Mir ist es zu wenig, wenn ich auf der einen Seite höre: Es gibt doch auch eine ganze Reihe von technischen Möglichkeiten, Sicherheit in Systeme, in Kommunikationssysteme, in Datenverarbeitungssysteme von vornherein mit zu implementieren oder ggf. nachzubessern. Das setzt natürlich voraus, dass das Bewusstsein, die Sensibilität genügend verbreitet ist, dieses zu tun, und zwar sowohl bei den Herstellern, bei den Produzenten, bei den Providern und natürlich auch beim Endnutzer. Mir scheint hier noch ein weites Feld an Möglichkeiten zu bestehen.

Wir werden und müssen selbstverständlich – jetzt komme ich auf das Stichwort „Cyberterrorismus“ oder „Cyberkriminalität“ – natürlich auch versuchen, uns durch Szenarienbildung auf Möglichkeiten vorzubereiten und einzustellen. Dies kann die Polizei nicht alleine. Dazu brauchen wir den Sachverstand der Hersteller, der Provider und natürlich auch des Bundesamts für die Sicherheit in der Informationstechnik.

Ich habe hier von dieser Tagung mitgenommen eine große Bereitschaft der Zusammenarbeit, des Gesprächs. Ich möchte das gerne aufgreifen. Das Bundeskriminalamt wird dazu entsprechende Initiativen einleiten. Alles in allem glaube ich, haben wir eine Fülle von Anregungen erhalten. Wir müssen uns möglicherweise mit dem Gedanken auseinander setzen, dass manches, was wir unter Sicherheitsgesichtspunkten, unter Strafverfolgungsgesichtspunkten für erforderlich und notwendig halten als Polizei, dass dieses aufgrund der technischen Entwicklung, die uns davonrennt, nicht mehr möglich ist. Herr Müller-Maguhn, Sie haben diesen Punkt angesprochen. Was mich nicht befriedigt, ist eine Aussage, die dahin geht, das Internet ist gekennzeichnet und soll gekennzeichnet sein durch ein Höchstmaß an Freiheit. Und weil das so ist und weil es ohnehin schwierig ist oder gar unmöglich ist, irgendwelche technische oder menschliche Prävention einzubauen, sollte man es laufen lassen, wie es ist. Das scheint mir unbefriedigend zu sein. Ich bin jedenfalls als Nichttechniker nicht so weit zu resignieren und zu sagen: Da ist wohl nichts mehr zu machen. Im Gegenteil. Erfolge, über die auch hier in der

Arbeitstagung berichtet worden sind, zeigen, dass wir sicherlich nicht in der Breite Erfolge vorweisen können, gemessen an der Fülle von Informationen, die Tag für Tag über die neuen Kommunikationstechnologien gehen. Aber ich denke, in punktuellen, auch etwas breiter angelegten Bereichen haben wir die Erfolge. Und daran müssen wir weiter arbeiten.

Ich bedanke mich für Ihr Kommen. Ich hoffe, Sie gehen mit einigen Anregungen zurück an Ihre Arbeitsstätten. Vielen Dank den Referenten für Ihre Mitwirkung! Vielen Dank der Technik des Hauses, den Organisatoren! Herr Dr. Stock, es lag in Ihren Händen.

Ich wünsche Ihnen eine gute Heimfahrt und würde mich freuen, Sie im nächsten Jahr zu unserer 50. Arbeitstagung hier in Wiesbaden wieder begrüßen zu können.

Auf Wiedersehen!

Über die Referenten*

Brunnstein, Klaus, Prof. Dr. rer. nat.

Professor für Anwendungen der Informatik an der Universität Hamburg (seit 1973); 1964 Dissertation in Physik/Angewandter Mathematik am Institut für Schiffbau der Universität Hamburg; Mitarbeiter am Rechenzentrum Deutsches Elektronen-Synchrotrons (DESY) in Hamburg (1965–1973); Mitglied der Gründungskommission des Studienganges Informatik der Universität Hamburg (seit 1969); von Januar bis April 1983 beurlaubt als nachgerücktes Mitglied des Deutschen Bundestages; 1988 Gründung des „Virus Test Centers" (VTC); zahlreiche Funktionen in internationalen Gremien, u. a. in der International Federation for Information Processing (IFIP) im Technical Committee TC-9 „Computers and Society"; 1990 bis 1995 dessen Vorsitzender; deutscher Vertreter (GI) in IFIP Generalversammlung (General Assembly) (seit 1999); 2000 Wahl zum IFIP Vice President; 2002 Wahl zum (14.) IFIP President (Amtszeit: 2002–2004); Arbeitsschwerpunkte u. a.: Risikoanalyse und Notfallvorsorge computer-gestützter Systeme, Technologie-Folgen-Abschätzung; zahlreiche wissenschaftliche Veröffentlichungen.

Prof. Dr. Klaus Brunnstein
Universität Hamburg
Vogt-Kölln-Straße 30
22527 Hamburg

Dix, Alexander, Dr. jur.

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg (seit Juni 1998); 1969 bis1977 Studium der Rechtswissenschaften in Bochum, Hamburg und London; 1977 Masters of Laws (LL. M.) – University of London; 1980 bis 1982 Wissenschaftlicher Referent am Hans-Bredow-Institut für Rundfunk und Fernsehen an der Universität Hamburg; 1984 dort Promotion zum Dr. jur.; Juristischer Referent bei der Stadt Heidelberg (1982–1985) sowie beim Berliner Datenschutzbeauftragten (1985–1990); 1990 bis 1998 Stellvertretender Berliner Datenschutzbeauftragter.

Dr. Alexander Dix
Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

* Stand: Dezember 2003

Finn, David

Director of Digital Integrity für Europa, den Nahen Osten und Afrika (EMEA) von Microsoft mit Sitz in Paris, Leiter eines internationalen Teams ehemaliger Vertreter von Strafverfolgungsbehörden, Ermittlern und Anwälten; für Microsoft in diesem Bereich federführend in der Bekämpfung der organisierten Kriminalität im Bereich Fälschung und anderer Formen der Kriminalität unter Nutzung des Internet, einschließlich Virusverbreitung, Identitätsdiebstahl und Hacking; Absolvent des Harvard College und der Harvard Law School mit Auszeichnung; als Assistant United States Attorney (stellvertretender Bundesanwalt) in New York City enge Zusammenarbeit mit verschiedenen US-amerikanischen Strafverfolgungsbehörden auf Bundesebene und auf lokaler Ebene, u. a. mit FBI, DEA, Secret Service, ATF und der New Yorker Polizei; als Staatsanwalt Anklagevertreter unterschiedlichster Gewalttaten und Wirtschaftsstraftaten an US-Bezirks- und Berufungsgerichten; seit Beginn seiner Tätigkeit bei Microsoft im Jahr 1999 regelmäßige Zusammenarbeit mit Staatsanwälten und Vertretern von Sicherheitsbehörden in ganz Europa.

David Finn
Microsoft
Tour B la Defense
F-92932 Paris la Defense

Glotz, Peter, Prof. Dr. phil.

Professor für Kommunikationswissenschaft und Direktor am Institut für Medien- und Kommunikationsmanagement der Universität St. Gallen und Direktor des Executive MBA in Media and Communication; in den 60er Jahren wissenschaftlicher Assistent am Institut für Kommunikationswissenschaft der Universität München; Konrektor der Universität München (1969–1970); Geschäftsführer einer Firma für Kommunikationsforschung (1970–1972); später 26 Jahre politische Tätigkeit, darunter Staatssekretär im Bundesbildungsministerium (1974–1977), Senator für Wissenschaft und Forschung Berlin (1977–1981), Bundesgeschäftsführer der SPD (1981–1987); 12 Jahre Senator der Max-Planck-Gesellschaft, Mitglied des Stiftungsrats des Wissenschaftskollegs zu Berlin; 1991 Gastprofessor Marquette Universität Milwaukee; 1993 Honorarprofessor für Kommunikationskultur und Medienökologie an der Universität München; 1996–1999 Rektor der Universität Erfurt. Ständiger Gastprofessor und Direktor ab Januar 2000 am Institut für Medien und Kommunikationsmanagement der Universität St. Gallen und Direktor des Executive MBA in Media and Communication. Zwischen Februar und Oktober 2002 Beauftragter des Bundeskanzlers für den EU-Konvent zur Ausarbeitung einer europäischen Verfassung. Vielfältige Buch- und Zeitschriftenveröffentlichungen zur Kommunikationswissenschaft, Bildungspolitik, Politischen Theorie, darunter drei politische Tagebü-

cher; Mitglied des Verbands Deutscher Schriftsteller und des Deutschen PEN (West).

Prof. Dr. Peter Glotz
Universität St. Gallen
Blumenbergplatz 9
CH-9000 St. Gallen

Günther, Ralf

Oberstaatsanwalt bei der Generalstaatsanwaltschaft Celle, Referent der Zentralen Stelle „Organisierte Kriminalität und Korruption" (ZOK) (seit Februar 2001); dort neben der Bearbeitung von Rechtsbeschwerde-, Revisions- und Auslieferungssachen etc. in erster Linie zuständig für die Bearbeitung von Grundsatzfragen im Zusammenhang mit Organisierter Kriminalität, insbesondere strafprozessuale Ermittlungsmaßnahmen einschließlich des gesamten Bereichs der verdeckten Ermittlungen und des Telekommunikationsüberwachungsrechts; Studium der Rechtswissenschaften an den Universitäten Saarbrücken, Freiburg und Göttingen; 1992 Eintritt in den Justizdienst des Landes Berlin; dort zunächst tätig als planmäßiger Dezernent in einem Dezernat zur Bekämpfung der Organisierten Kriminalität mit Schwerpunkt „Internationale Kfz-Verschiebung"; anschließend Tätigkeit als Dezernent in der allein zu diesem Zweck eingerichteten Staatsanwaltschaft II bei dem Landgericht Berlin „Verfahren im Zusammenhang mit der Regierungs- und Vereinigungskriminalität"; 1996 Wechsel zur Staatsanwaltschaft Hannover und Tätigkeit in den Abteilungen zur Bekämpfung der Organisierten Kriminalität sowie in der Zentralstelle zur Bekämpfung von Betäubungsmittelstrafsachen; 2000 vorübergehend als Dezernent bei der Staatsanwaltschaft Göttingen.

Ralf Günther
Generalstaatsanwaltschaft Celle
Schloßplatz 2
29221 Celle

Heidemann-Peuser, Helke

Leiterin des Referats Wirtschaftsrecht im Verbraucherzentrale Bundesverband e. V. (seit 2001); Studium der Rechtswissenschaften an der Rheinischen Friedrich-Wilhelms-Universität Bonn (1972–1978); 1978 Erstes juristisches Staatsexamen an der Johannes-Gutenberg-Universität Mainz; Referendarausbildung beim Kammergerichtspräsidenten in Berlin (1978–1981); 1981 Zweites juristisches Staatsexamen in Berlin; 1981 bis 1983 Referentin für Wettbewerbsrecht im Verbraucherschutzverein e. V. in Berlin; 1983 bis 2001 Leiterin der Abteilung „Allgemeine Geschäftsbedingungen" im Verbraucherschutzverein; diverse Veröffentlichungen in Fachzeitschriften, insbesondere zum Recht der Allgemeinen Geschäftsbedingungen sowie zum Klagerecht der Verbraucherverbände nach

Artikel 1 § 3 Nr. 8 RBerG in „Verbraucher und Recht“ (VuR), ferner zur Zulässigkeit von Datenschutzklauseln in „Datenschutz und Datensicherheit“ (DuD), Kommentierung des Unterlassungsklagengesetzes im Praxiskommentar zur Schuldrechtsmodernisierung.

Helke Heidemann-Peuser
Verbraucherzentrale Bundesverband
Markgrafenstr. 66
10969 Berlin

Helmbrecht, Udo, Dr. rer. nat.

Präsident des Bundesamtes für Sicherheit in der Informationstechnik in Bonn (seit März 2003); nach Studium der Physik und Mathematik an der Ruhr-Universität Bochum 1981 Abschluss als Diplom-Physiker; 1984 Promotion zum Dr. rer. nat.; 1981 bis 1983 wissenschaftlicher Angestellter am Institut für theoretische Physik der Ruhr-Universität Bochum; danach bis 1985 Tätigkeit als Abteilungsleiter Anwendungssoftware an der Bergischen Universität Wuppertal. 1985 Wechsel zu Messerschmitt-Bölkow-Blohm (heute EADS) nach München, dort tätig in unterschiedlichen Leitungsfunktionen (Projektleiter, Assistent, Abteilungsleiter, Programmleiter) und in internationalen Projekten (USA, China); in diesen Funktionen verantwortlich für die softwaretechnische Unterstützung der Flugzeugentwicklung, -konstruktion und -fertigung. 1995 Eintritt in den Dienst der Bayerischen Versorgungskammer als Direktor und Bereichsleiter Informationsverarbeitung und unter seiner Verantwortung Entwicklung dieses Bereichs zu einem anerkannten, kostengünstigen und effizienten IT-Dienstleister. Hervorzuheben sind unter anderem das Hochverfügbarkeits-Rechenzentrum, die flächendeckende PC-Vernetzung, der Jahrtausendwechsel und die Euro-Einführung sowie der Systemwechsel in der Zusatzversorgungkasse ZkdbG. Bei Schwerpunktsetzung auf unternehmerisches Denken in einer Behörde unter anderem Förderung von Themen wie IT-Qualitätsmanagement, IT-Sicherheit, IT-Balanced Scorecard.

Dr. Udo Helmbrecht
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185–189
53175 Bonn

Hynds, Len

Detective Chief Superintendent und Erster Leiter der National Hi-Tech Crime Unit mit Zuständigkeit für die Entwicklung und Umsetzung eines Centre of Excellence zur Bekämpfung der Hi-tech Kriminalität und die Erarbeitung von Benchmark-Standards für alle Dienststellen zur Bekämpfung der Computerkriminalität in England und Wales (seit 2001); vorwiegend Ermittlungstätigkeit im operativen Bereich mit Schwerpunkt Schwerkriminalität und organisierte Kri-

minalität; Einsatz im taktischen, strategischen und Grundsatzbereich in mehr als 30 Ländern; in Partnerschaft mit ausländischen Kollegen Zerschlagung von international agierenden Straftäterorganisationen und Optimierung der Ermittlungstätigkeit; Berater der Regierung bei Gesetzesinitiativen, Teilnehmer an Sitzungen der UN-Drogenkommission mit Beraterstatus für die britische Delegation und Leiter EU-finanzierter Workshops zur Harmonisierung der Maßnahmen der Strafverfolgungsbehörden; Mitbegründer der National Crime Squad; gilt als Architekt des Zusammenarbeitsübereinkommens zwischen der National Crime Squad und HM Customs and Excise; Vorsitzender des UK Internet Crime Forum, das Strafverfolgungsbehörden und Industrie an einen Tisch bringt, um partnerschaftliche Lösungen zur Bekämpfung der Hi-Tech Kriminalität u. ä. zu erarbeiten, sowie der Association of Chief Police Officers National Hi-Tech Crime Working Group, deren Ziel die Entwicklung von Standards bei Ermittlungen auf dem Gebiet der Hi-Tech Kriminalität ist.

Len Hynds
NHTCU
PO Box 10101
London E14 9NF

Kersten, Klaus Ulrich, Dr. jur.

Präsident des Bundeskriminalamtes (seit April 1996); 1961 bis 1965 Studium der Rechtswissenschaften; 1970 bis 1972 Bundesministerium des Innern, Referat „Olympische Spiele München"; 1972 Bundesamt für Verfassungsschutz; 1972 bis 1973 Grenzschutzdirektion Koblenz; Ende 1973 bis 1996 Bundesministerium des Innern; zunächst Referat für „Innerdeutsche und Berlin-Angelegenheiten"; 1976 bis 1978 Abteilung Polizeiangelegenheiten, Referat „Allgemeine kriminalpolizeiliche Angelegenheiten"; 1978 bis 1980 Arbeitsgruppe „Allgemeine Angelegenheiten des Bundeskriminalamtes und der Verbrechensbekämpfung"; 1980 bis 1987 Leiter des Referates „Polizeiliches Informationswesen; Kriminaltechnik"; 1987 bis 1991 Leiter des Referates „Grundsatz-, Rechts- und Organisationsangelegenheiten des Bundesgrenzschutzes"; 1991 bis Anfang 1995 Leiter der Unterabteilung „Allgemeine Polizeiangelegenheiten; allgemeine Angelegenheiten des BGS"; 1995 bis März 1996 Leiter der neu gebildeten Abteilung „Bundesgrenzschutz"; Januar bis Juni 1999 für die Dauer der deutschen Präsidentschaft der Europäischen Union Übernahme der Funktion des Abteilungsleiters „Polizeiangelegenheiten" im Bundesministerium des Innern; seit November 2000 in seiner Eigenschaft als Präsident des Bundeskriminalamtes Delegierter für Europa im Exekutivkomitee der IKPO-Interpol.

Dr. Klaus Ulrich Kersten
Bundeskriminalamt
Thaerstraße 11
65193 Wiesbaden

Kienzle, Ulrich

Studium der Politischen Wissenschaften in München und Tübingen. Weitere Fächer: Germanistik und Kunstgeschichte; 1956 bis 1967 Tätigkeit beim SDR Stuttgart, zuerst als freier Reporter, später als festangestellter Redakteur der „Abendschau"; in der Zeit von 1967 bis 1968 Wechsel zum WDR, dort Mitarbeit im FS-Magazin „Zum Tage", danach Rückkehr zum SDR und Chef der „Abendschau Baden-Württemberg"; 1972 bis 1974 Redaktion/Moderation des gemeinsam von SDR und BR ausgestrahlten Auslandsmagazins „Kompass" zusammen mit Dagobert Lindlau; ARD-Korrespondent für Arabien in Beirut (1974–1977) sowie für das Südliche Afrika (1977–1980); Chefredakteur Fernsehen bei Radio Bremen (1980–1990); Leiter der HR Außenpolitik im ZDF und Moderator des „auslandsjournal" (1990–1993); Leiter und Moderator des wöchentlichen ZDF-Magazins „FRONTAL" (1993–2000); seit 1997 Leiter und Moderator der ZDF-Sendung „Hauser & Kienzle u. die Meinungsmacher" sowie (2002) Leiter und Moderator der ZDF Sendung „Machtduell" zur Bundestagswahl 2002; zahlreiche Veröffentlichungen und Auszeichnungen.

Ulrich Kienzle
Zweites Deutsches Fernsehen
ZDF-Straße 1
55100 Mainz

Kindler, Waldemar

Abteilungsleiter „Öffentliche Sicherheit und Ordnung" im Bayerischen Staatsministerium des Innern (seit März 2001); Studium der Rechtswissenschaften an der Universität München; anschließend wissenschaftlicher Mitarbeiter am Institut für Arbeits- und Wirtschaftsrecht der Universität München; 1975 Eintritt in die Bayerische Polizei; Tätigkeiten im Polizeipräsidium München als Sachbearbeiter für Rechtsangelegenheiten (1975–1983), Leiter des Sachgebietes Rechtsangelegenheiten (1983–1984), Personalchef des Polizeipräsidiums München (1984–1987), im Bayerisches Staatsministerium des Innern (1987–1989); Vizepräsident des Bayerischen Landeskriminalamtes (1989–1992); im Bayerischen Staatsministerium des Innern Leiter des Sachgebietes Einsatz, Organisation und Dienstbetrieb (1992–1993); Personalchef der Bayerischen Polizei und zugleich stellvertretender Leiter der Abteilung Öffentliche Sicherheit und Ordnung (1993–2001).

Waldemar Kindler
Bayerisches Staatsministerium des Innern
Odeonsplatz 3
80539 München

Königshofen, Thomas

Stellvertretender Leiter Konzernsicherheit der Deutschen Telekom, verantwortlich für das Lage-, Informations- und Krisenmanagement sowie den Personen-, Veranstaltungs- und Objektschutz im Konzern (seit 2002); Studium der Rechts- und Wirtschaftswissenschaften in Münster und Bonn; nach dem 2. jur. Staatsexamen Tätigkeit als Assistent des Dekans der Rechtswissenschaftlichen Fakultät der WWU Münster; 1988 Eintritt bei der Deutschen Bundespost, dort mit verschiedenen Managementfunktionen in Niederlassungen betraut, zuletzt als Leiter einer Niederlassung; 1989 Wechsel in das Bundesministerium für Post und Telekommunikation, dort Mitarbeit an den Gesetzesentwürfen zur Postreform I; 1990 Wechsel zur Deutschen Telekom, dort in der Rechtsabteilung der Zentrale zuständig für nationales und internationales Telekommunikationsrecht sowie Vertragsrecht; ab 1992 Fachbereichsleiter für Datenschutz, Informationssicherheit und Strafrecht und Datenschutzbeauftragter der Deutschen Telekom AG; von 1999 bis 2002 Konzerndatenschutzbeauftragter des Konzerns Deutsche Telekom. Zahlreiche Vorträge und Veröffentlichungen in den Fachgebieten Telekommunikationsrecht, Datenschutz, Informationssicherheit sowie Notfall- und Krisenmanagement in der IT.

Thomas Königshofen
Deutsche Telekom
Friedrich-Ebert-Allee 140
53113 Bonn

Kossel, Axel

Leiter des Ressorts „Internet“ beim c’t magazin (seit 1994); 1986 Unterbrechung des Informatik-Studiums für zwei Praxissemester als Volontär beim Verlag Heinz Heise in Hannover; nach verkürztem Volontariat 1988 Tätigkeit als Redakteur für das c’t magazin. Als technisch orientiertes Magazin für Anwender und Profis kümmert sich c’t nicht nur um die Technik, sondern auch um deren politische, juristische und gesellschaftliche Auswirkungen.

Axel Kossel
Magazin c’t
Helstorfer Str. 7
30625 Hannover

Müller-Maguhn, Andy

Betreibt seit Mitte 2002 in Berlin unter der Bezeichnung „Datenreisebüro“ ein Bürogebäude, das neben dem Chaos Computer Club Berlin auch Workshop- und Archivräume umfasst und derzeit mit der Konzeption von Schulungen und Workshops versucht, die unterschiedlichsten Erfahrungen, insbesondere im Be-

reich von Datenschutz und Datensicherheit, zur Gestaltung von Policies und Strukturen nutzbar zu machen. Seit 1986 Mitglied im Chaos Computer Club, befasst mit den verschiedenen technischen und gesellschaftlichen Aspekten der Informations- und Kommunikationstechnologie, insbesondere den Auswirkungen von Netzarchitekturparametern auf die Kommunikationsräume. Bereits während des Studiums der Nachrichtentechnik und Informationswissenschaft tätig als Journalist, Berater und Sachverständiger im Bereich elektronischer Netzwerke. Von Ende 2000 bis Mitte 2003 von Internetnutzern gewählter ehrenamtlicher Direktor von ICAAN (Internet Corporation for Assigned Names and Numbers) mit 18 anderen Direktoren zusammen für die weltweite Entwicklung von Richtlinien und der Entscheidung über strukturelle Fragen der weltweiten Internet-Struktur zuständig. Seit Juni 2002 tätig als ehrenamtliches Vorstandsmitglied der European Digital Rights (EDRI), der sich als Dachverband europäischer NGO's für die Durchsetzung der Menschenrechte auch im Digitalzeitalter einsetzt. Durch die ehrenamtliche Tätigkeit als Vorstandsmitglied und Sprecher im Chaos Computer Club Betreuung von Projekten des schöpferisch kritischen Umgangs mit Technologie und ihren Auswirkungen auf die Konzeption zukunftsfähiger Strukturen. Dabei steht das Prinzip der Transparenz der Technologie und der Beachtung sozialer und gesellschaftlicher Auswirkungen im Vordergrund.

Andy Müller-Maguhn
CCC Berlin
Postfach 64 02 34
10048 Berlin

Ratzel, Max-Peter

Abteilungspräsident, Leiter der Abteilung OA (Organisierte und Allgemeine Kriminalität) im Bundeskriminalamt (seit 2000); 1976 Eintritt in das Bundeskriminalamt; 1980 bis 1985 Verwendungen als Beamter des gehobenen Dienstes in den Bereichen „Nachrichtenaustausch Rauschgiftkriminalität", „Auswertung Rauschgiftkriminalität", „Ermittlungen Rauschgiftkriminalität" und „polizeifachliche Grundsatzfragen der polizeilichen Datenverarbeitung"; 1985 bis 1987 Ausbildung zum höheren Kriminaldienst; anschließend (1987 bis 1998) Referent im Leitungsstab für Grundsatzfragen polizeilicher Informationstechnik und sonstiger Technik, Referent im Fachreferat für Grundsatzfragen zur OK, Kommissarische Leitung eines Referates für OK-Ermittlungen, Referatsleiter „Allgemeine Eigentumskriminalität", Leitungsassistent für einen Hauptabteilungsleiter sowie Referatsleiter „Internationale Zusammenarbeit – Grundsatz". 1998 Leiter des Leitungsstabes der Amtsleitung.

Max-Peter Ratzel
Bundeskriminalamt
Thaerstraße 11
65193 Wiesbaden

Rheinboldt, Jörg

Geschäftsführer der eBay GmbH als Trust & Safety (gemeinsam mit dem Vorsitzenden der Geschäftsführung Philipp Justus und Dr. Stefan Groß-Selbeck). Studium der Betriebswirtschaftslehre an der Universität Köln mit Schwerpunkt Marketing und Internationales Management; als Mitglied des Organisationsforums Wirtschaftskongress (OFW) während des Studiums Leitung der Akquisition der Referenten für den Deutschen Wirtschaftskongress „Mehrwert Information", an dem unter anderem Bill Gates und Mark Wössner vortrugen; Einstieg ins Berufsleben als Gründer der Multimedia-Agentur Denkwerk Neue Medien Holding GmbH; als Geschäftsführer und Projektmanager bei Denkwerk Betreuung namhafter Kunden der deutschen Wirtschaft wie Henkel, Sal. Oppenheim, IHK Köln und Ritter Sport; danach (1999) Gründung der Alando AG, die im Mai 1999 mit dem Weltmarktführer eBay fusionierte und nachfolgend Aufbau von eBay Deutschland; Gründungsmitglied der NewMedia.Net Berlin-Brandenburg e. V.

Jörg Rheinboldt
eBay GmbH
Marktplatz 1
14532 Dreilinden

Schürholz, Franz-Hellmut

Präsident des Landeskriminalamtes Baden-Württemberg (seit 1992); nach 1. und 2. Juristischem Staatsexamen ab 1974 Tätigkeiten in der Landesverwaltung Baden-Württemberg, in einem Landratsamt, im Sozialministerium und im Innenministerium als Leiter des Referats „Recht und Grundsatzangelegenheiten der Polizei" sowie als Stellvertreter des Landespolizeipräsidenten.

Franz-Hellmut Schürholz
Landeskriminalamt Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart

Schütte, Jürgen

Hauptdezernent für ordnungsrechtliche Aufgaben und Dezernent für Medienaufsicht bei der Bezirksregierung Düsseldorf; dort bereits seit 1982 in verschiedenen Aufgabenbereichen beschäftigt. Erstes und Zweites Juristisches Staatsexamen in Hamburg. Juristischer Autor der „Düsseldorfer Sperrverfügungen".

Jürgen Schütte
Bezirksregierung Düsseldorf
Cäcilienallee 2
40474 Düsseldorf

Tagungsleitung

Stock, Jürgen, Prof. Dr. jur.

Abteilungspräsident, Leiter der Abteilung „Kriminalistisches Institut“ des BKA.

Prof. Dr. Jürgen Stock
Bundeskriminalamt
Thaerstr. 11
65193 Wiesbaden