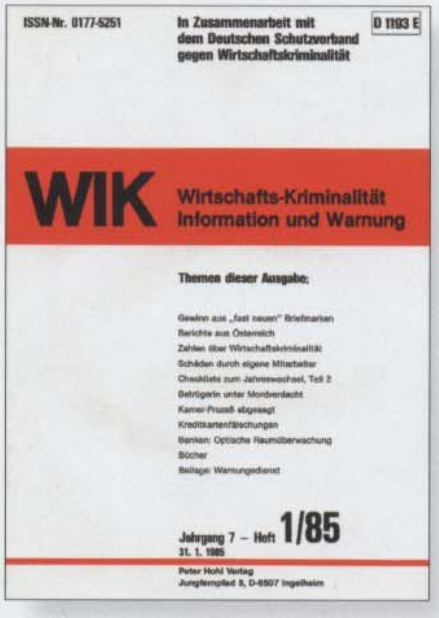
Jubiläumsausgabe, Sondernummer September 2003

1193
ISSN-Nr. 1615-455X

WIK

Zeitschrift für die Sicherheit der Wirtschaft

Fünfundzwanzig Jahre Sicherheitsgeschichte, Chroniken, Design, Jubilare, Ausblicke und Rückblenden



25 Jahre für die Sicherheit

SecuMedia Verlags-GmbH, Postfach 1234, D-55205 Ingelheim
Postvertriebsstück · Entgelt bezahlt · 1193

AUTOREN VON A BIS Z

Seite 17
Dipl.-Ing. Gerhard M. Beier ist freier Consultant und berät im Rahmen seines „Technologie Transferzentrum Saar" in Sicherheitsfragen zum Thema „IT und Technologie-Transfer". Er war bis in die 80er Jahre Mitarbeiter des DDR-Auslandsnachrichtendienstes und hatte in der Bundesrepublik und dem benachbarten Ausland als Offizier im besonderem Einsatz eigene Agenten geführt.
Kontakt: Ewivlux@aol.com

Seite 87
Dieter Gartenschläger ist seit 1967 in vielfältigen Funktionen für die Winkhaus-Gruppe, Münster, tätig, zuletzt als Vertriebsleiter Sicherheitssysteme, im Bereich Fachhandel und aktuell als Berater. Kontakt: dieter.gartenschlaeger@t-online.de

Seite 41
Klaus-Henning Glitza ist freier Journalist, Autor und Mitglied des VSW Niedersachsen. Sein Spezialgebiet sind Themen aus der Sicherheit. Kontakt: khglitza@t-online.de

Seite 14
Oberst Roland Kaestner ist Leiter „Strategische Zukunftsanalysen" im Zentrum für Analysen und Studien der Bundeswehr, Waldbröl, und beschäftigt sich seit mehr als zehn Jahren mit strategischen Fragen der äußeren Sicherheit, unter anderem 1999/2000 als Mitarbeiter der Bundestagsfraktion von Bündnis 90/die Grünen. Sein Beitrag ist eine Kurzfassung eines Vortrags, den der Autor anlässlich der diesjährigen Sicherheitstagung des Bayerischen Verbands für Sicherheit in der Wirtschaft gehalten hat. Kontakt:
RolandKaestner@ bundeswehr.org

Seite 32
Patrick Keil ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Software und Systems Engineering der Technischen Universität München, an der die Studie „Kommunikations- und Informationstechnik 2010+3" entstand und an der er als Mitautor fungierte. Zu seinen Arbeitsschwerpunkten gehören die Trendforschung in der IT sowie Business Information Systems. Kontakt:
keilp@informatik.tu-muenchen.de

Seite 70
Irene Kölbl und **Stefan Wagner** bilden das KÖWA-TEAM (Redaktionsbüro und Bildagentur), Berlin. Sie arbeiten seit mehreren Jahren als freie Fachjournalisten für die WIK, unter anderem im Bereich Sicherheitstechnik. Kontakt: irene.koelbl@ber.netsurf.de

Seite 27
Michael Otto verantwortet im Sicherheitsberatungsunternehmen Kroll Deutschland, Frankfurt Main, für den deutschen Sprachraum den Bereich Risiko- und Sicherheitsmanagement. Kontakt: Tel. 069 768070

Seite 37
Stephan Löw ist Marketing & Sales Manager bei De La Rue Cash Systems GmbH. Seit Mai 2002 verantwortet er den Marketingbereich des Unternehmens.
Kontakt: stephan.loew@de.delarue.com

Seite 76
Dr. Thomas M. Mann (li.) ist Leiter Business Support Fire Safety bei der Siemens Gebäudetechnik GmbH & Co. oHG, München.
Kontakt: Thomas.M.Mann@siemens.com
Helmut Macht ist Chief Technology Officer bei der Siemens Building Techologies AG, Zürich.
Kontakt: Helmut.Macht@siemens.com

Seite 92
Dr. Harald Olschok ist Hauptgeschäftsführer des Bundesverbandes Deutscher Wach- und Sicherheitsunternehmen (BDWS).
Kontakt:
Tel. 06172 948050

Seite 54
Klaus Rosenbaum ist seit 1974 Leiter Arbeits- und Werksicherheit der WMF AG, Geislingen, einem renommierten Hersteller von Bestecken, Kochgeschirren, Servicegeräten, Schneidwaren und gewerblichen Kaffeemaschinen. Der international tätige WMF-Konzern beschäftigt ca. 5.400 Mitarbeiter.
Kontakt: Tel. 07331 25-0

Seite 44
MinDir a.D. Reinhard Rupprecht war bis zu seinem Wechsel in den Ruhestand Leiter der Abteilung für Innere Sicherheit im Bundesministerium des Innern. Heute unterstützt er als Mitarbeiter die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) und arbeitet als freier Berater und Autor.
Kontakt: Rerupprecht@aol.com

Seite 29
Dr. phil. Henning Schmidt-Semisch ist Privatdozent im Fachbereich 11 der Universität Bremen. Sein Beitrag „Überlegungen zu einer Kriminalitätsversicherung" beruht auf seiner Habilitationsschrift „Kriminalität als Risiko. Schadenmanagement zwischen Strafrecht und Versicherung", für die der Dipl.-Kriminologe und Soziologe (MA) in 2002 den zweijährlich vergebenen Fritz-Sack-Preis für Kriminologie erhalten hat.
Kontakt: schmidt-semisch@uni-bremen.de

Seite 23
Michael H. Sorge ist Leiter des Bereiche RK-Corporate Security der Bayer AG, Vorsitzender des Verbandes für Sicherheit in der Wirtschaft Nordrhein-Westfalen und stellvertretender Vorsitzender der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW). Kontakt: Tel. 0214 3028937

Seite 49
Wolfgang Wipper ist Vorsitzender des Bayerischen Verbands für Sicherheit in der Wirtschaft e.V. (BVSW) und verantwortet seit 1979 in unterschiedlichen Funktionen den Werkschutz bei Siemens in der Region München. Heute ist er Leiter des Sicherheits- und Veranstaltungsdienstes im Bereich Siemens Real Estate München.
Kontakt: Tel. 089 722-47900

AUTOREN VON A BIS Z

Entwicklungslinien der IT-Sicherheit

BSI-Studie: Akzeptanz für Sicherheitslösungen wächst langsam

Die zunehmende Abhängigkeit von komplexeren Systemen der Informations- und Kommunikationstechnik (IuK) stellt uns ständig vor neue Herausforderungen hinsichtlich deren Sicherheit. Schlagworte wie Web-Services, Mobilität oder Telearbeit verdeutlichen den Rahmen, in dem über das Angreifen, Stören und Blockieren von einzelnen Anwendungen und komplexen Systemen diskutiert wird. Solchen Bedrohungen durch entsprechende Schutzmaßnahmen entgegen zu wirken, wird künftig zu einer Hauptaufgabe der IuK-Sicherheit. Diese Aufgabe ist vielschichtig und berührt neben organisatorischen und personellen Aspekten ein breites Spektrum technologischer Möglichkeiten aus unterschiedlichen Disziplinen.

Von Patrick Keil, München

Um diese Möglichkeiten und die beschriebenen Gefahren besser einschätzen zu können, entstand im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Studie „Kommunikations- und Informationstechnik 2010+3", die Trends in der IuK der nächsten zehn Jahre evaluiert und dabei ein besonderes Augenmerk auf Sicherheitsaspekte legt. Alle nicht eigens gekennzeichneten Ergebnisse in diesem Beitrag entstammen dieser im Mai vorgestellten Studie.

Vermehrte Anstrengungen sind nötig, denn:

■ Immer mehr Unternehmen arbeiten an einer integrierten, mehrere Prozesse und Bereiche umspannenden IT-Infrastruktur. Je komplexer die Systeme, desto vielschichtiger die Sicherheitsanforderungen und desto größer die Menge und die Bedeutung der gehaltenen Daten.

■ Mobile Dienste werden verstärkt auch zum Datentransfer genutzt. Die Zunahme der schnurlosen Kommunikation bedeutet auch neue Risiken: zum einen sind mobile Geräte leichter zu entwenden als stationäre. Wichtiger ist allerdings die Frage, wie das Abhören von Gesprächen sowie das Abfangen von Daten verhindert werden kann. Dies ist für die gängigen Technologien (Bluetooth, UMTS etc.) noch nicht ausreichend sichergestellt.

■ Die Computer-unterstützte Zusammenarbeit mehrerer Unternehmen (Supply Chain Management, e-Procurement etc.), der gemeinsame Zugriff auf Daten im Unternehmen (File Sharing) sowie die Verbreitung von Web Services werfen Fragen nach Vertraulichkeit und Unversehrtheit von Daten auf.

■ In einer wirtschaftlich labilen Lage müssen sich Unternehmen einerseits mit einem enormen Kostendruck, andererseits mit höheren Risiken durch das Ausspähen von Firmendaten auseinandersetzen.

Eine Reihe von Maßnahmen ist für die erfolgreiche Bekämpfung dieser (neuen und bisherigen) physischen und elektronischen Bedrohungen nötig:

■ Die akademische und betriebliche Aus- und Weiterbildung berücksichtigt Problemlagen und erforderliche Technologien noch zu wenig. Aspekte der IuK-Sicherheit müssen in den Lehrplänen so früh wie möglich verankert sein.

■ Es gibt zu viele Zertifikate, Siegel und Normen, was zu geringem Bekanntheitsgrad und mangelnder Akzeptanz führt. Die meisten werden auch hinsichtlich ihrer Anforderungen an Sicherheit als zu uneinheitlich und intransparent angesehen und/oder greifen aufgrund ihrer Orientierung an Entwicklungsmodellen zu kurz. Deshalb wird mit einer weiten Verbreitung solcher Gütesiegel und Zertifikate erst in fünf Jahren gerechnet, eine Bereinigung des Marktes wird allerdings noch geschätzte acht Jahre auf sich warten lassen. Das Sicherheitsniveau (stärker) in bestehende Zertifizierungen wie ISO 9000 zu integrieren, wäre vor diesem Hintergrund sinnvoll, die Aufnahme der IT-Sicherheit in die Unternehmensrevision scheint dagegen noch in weiter Ferne.

■ Politische Rahmenbedingungen müssen auch weiterhin der wichtigste Förderer der IuK-Sicherheit sein. Durch Regulierung können, wenn auch in begrenztem Umfang, das Problembewusstsein erhöht und Investitionen erzwungen werden. Wünschenswert ist, dass Behörden und staatliche Einrichtungen (wieder) als Vorreiter für den Einsatz neuer und umfassenderer Sicherheitsmaßnahmen fungieren. Auch – oder gerade – in der jetzigen wirtschaftlichen Situation müssen staatliche Förderungen und Forderungen als Investition in die Zukunft des Wirtschaftsstandortes gesehen werden.

■ Es besteht ein großer Handlungsbedarf hinsichtlich der Schaffung und Durchsetzung international einheitlicher Regeln und Standards. Die Vielzahl unterschiedlicher nationaler Rechtsgrundlagen, die für globalisierte, integrierte Wertschöpfungsketten und internationalen elektronischen Handel gelten, wirken als Hemmschuh für die gesamte wirtschaftliche Entwicklung. Gerade für die Sicherheit von Transaktionen und den Datenschutz müssen einheitliche, gemeinsame Regeln geschaffen werden.

■ Der Blick auf einzelne Sicherheitslösungen, die nachträglich installiert werden oder erst Berücksichtigung finden, wenn das zu schützende System bereits entwickelt ist, ist kurzsichtig.

Patrick Keil ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Software und Systems Engineering der Technischen Universität München.

Nötig ist eine Integration von Sicherheitsaspekten in allen Phasen der SW-Entwicklung. Beispielsweise enthält das V-Modell in seiner aktuellen Form von 1997 nur rudimentäre Forderungen und Umsetzungsrichtlinien für Safety (im V-Modell „Kritikalität" genannt) und Security. Die Weiterentwicklung des V-Modells 1997, die unter anderem an der Technischen Universität München erfolgt, integriert Safety sowie Test- und QS-Verfahren in jeder Phase der Systementwicklung (www.v-modell-200x.de). Aber auch in anderen gängigen Vorgehensmodellen sind Sicherheitseigenschaften bisher eher zufällig, zu spät im Entwicklungsprozess und/oder nicht durchgängig genug berücksichtigt. Und selbst das IT-Grundschutzhandbuch, das nur „Minimalanforderungen" formuliert, wird erst in drei Jahren weit verbreitet eingesetzt werden.

■ Unternehmen müssen zur Bewertung von IT-Risiken Methoden entwickeln, so wie es in anderen Bereichen bereits möglich und gängig ist. Dezidierte Risikoanalyse- und Risikominimierungsmethoden müssen eingesetzt werden, um Kosten (Investitionen) und Nutzen (geringere Risiken, niedrigere mögliche Kosten durch Schäden) zu beziffern. Nur so können Investitionen in die Sicherheit schon während der Entwicklung als auch nachträglich in bestehenden Systemen bewertet und unternehmensinterne Entscheidungen auf ein solides Fundament gestellt werden. Kurz: Sicherheit darf nicht länger als ad-hoc-Aufgabe und unnötiger Kostenblock gesehen werden, sondern muss ein integraler Bestandteil der Prozesse und Systeme von Unternehmen und Behörden werden.

Ein Beispiel für den oben angesprochenen Einfluss der Politik auf den Sicherheitsmarkt ist das 1997 verabschiedete Signaturgesetz (SigG), mit dem der Begriff der „qualifizierten elektronischen Signatur" eingeführt wurde. Dieser beschreibt die gesetzlichen Anforderungen an digitale Signaturen für den Einsatz in Bereichen, die üblicherweise der Schriftform bedürfen. Elektronische Signaturen ermöglichen den Schutz der Integrität und Authentizität elektronisch übermittelter Daten und bilden – zusammen mit der Verschlüsselungstechnik – die Voraussetzung für den sicheren Transfer von kritischen Informationen, zum Beispiel im e-Business. Der Trend ist eindeutig und zeigt eine erhebliche Bedeutungszunahme qualifizierter elektronischer Signaturen auf. Aber obwohl diese digitalen Signaturen für viele innovative Dienste wie rechtsverbindliche elektronische Vertragsabschlüsse essentiell sind, kann mit deren weiten Verbreitung erst gegen Ende des Jahrzehnts gerechnet werden. Die beiden anderen im SigG genannten Signaturarten, elektronische und fortgeschrittene elektronische Signatur, werden nur mittelfristig weiter an Bedeutung gewinnen.

Eine der Sicherheitstechnologien, die erst in den vergangenen Jahren in den Mittelpunkt des Interesses gerückt ist und für viele zukünftige Dienste als elementar angesehen wird, sind Public-Key-Infrastrukturen (PKI), die bei der Ver- und Entschlüsselung mit privaten beziehungsweise öffentlichen Schlüsseln arbeiten. Obwohl die Euphorie der vergangenen Jahre mittlerweile deutlich nachgelassen hat, wird mit einer baldigen Verbreitung gerechnet. Dabei wird sich der Einsatz von PKIs für Kommunikationsbeziehungen zwischen Behörden als erstes etablieren, gefolgt von Kommunikationsbeziehungen zwischen Unternehmen beziehungsweise zwischen Unternehmen und Behörden. In den Bereichen Kunde/Unternehmen sowie Bürger/Behörde wird mangels heute sichtbarer „Killerapplikationen" erst deutlich später mit dem Einsatz solcher Systeme gerechnet. Die im Rahmen von PKIs benötigten Verzeichnisdienste werden etwa zeitgleich verfügbar sein.

Public-Key-Infrastrukturen zur Behandlung qualifizierter elektronischer Signaturen, die für rechtsverbindliche elektronische Transaktionen essentiell sind, werden nach Ansicht der Befragten in sechs Jahren weit verbreitet sein. Etwa ein Viertel der Befragten sehen eine weite Verbreitung nicht vor zehn Jahren. Für diese Zeitspanne werden vor allem die hohen Anforderungen und der organisatorische Aufwand als Begründung aufgeführt.

Zur Durchsetzung von PKI-Systemen spielt die Interoperabilität (Integration und Kommunikation verschiedener Systeme) eine wichtige Rolle. Hierzu gehören insbesondere die verwendeten Zertifikatsformate. Hier geht der Trend klar in Richtung der hierarchisch orientierten X.509v3-Zertifikate beziehungsweise einem möglichen Nachfolger. PGP-Zertifikate, die eher an das Konzept des „Web of Trust" angelehnt sind, werden hingegen trotz der umfangreichen Fördermaßnahmen vornehmlich im privaten

und akademischen Bereich verbleiben.

Biometrie: Komfortable Identifizierung – mangelnde Akzeptanz

Einer der meist beachteten und dynamischsten Bereiche der IuK-Sicherheit ist die Biometrie. Sie beschäftigt sich mit der Erfassung und dem Vergleich individueller Merkmale einer Person (zum Beispiel Stimme, Auge, Fingerabdruck etc.) durch technische Systeme zur Identifizierung. „Elektronische Pförtner" sind genauso mögliche Anwendungen wie die Zugriffssicherung bei Mobiltelefonen oder die Identifikation am Geldautomaten. Die komfortable Identifikation „im Vorbeigehen" und die Ablösung der vielen persönlichen Passwörter und PINs zählen zu den großen Vorteilen dieser Verfahren. Trotzdem wird es noch geschätzte sieben Jahre dauern, bis sie für Anwendungen im Alltag akzeptiert werden. Insbesondere die Iriserkennung wird sehr skeptisch gesehen. Zu groß ist die Angst vor medizinischen Schäden beziehungsweise die psychologische Barriere. Langfristig die größte Bedeutung wird die Gesichtserkennung erlangen. Wie die Sprecherkennung entspricht sie dem natürlichen menschlichen Identifizierungsverhalten. Im Moment sind allerdings die Technologien für beide Methoden noch nicht vollständig ausgereift.

Konkrete Anwendung wird die Biometrie in der Authentisierung mittels mobiler persönlicher Endgeräte (in sechs Jahren) oder mittels Chipkarten (in sieben Jahren) finden. Massenanwendungen, beispielsweise EC-Karten mit biometrischen Merkmalen, werden trotz vereinzelter Pilotprojekte in den nächsten zehn Jahren nicht erwartet. Auch hier könnte der Staat Wegbereiter sein, beispielsweise durch die bereits diskutierte Einführung von Ausweisen, die derartige Merkmale speichern.

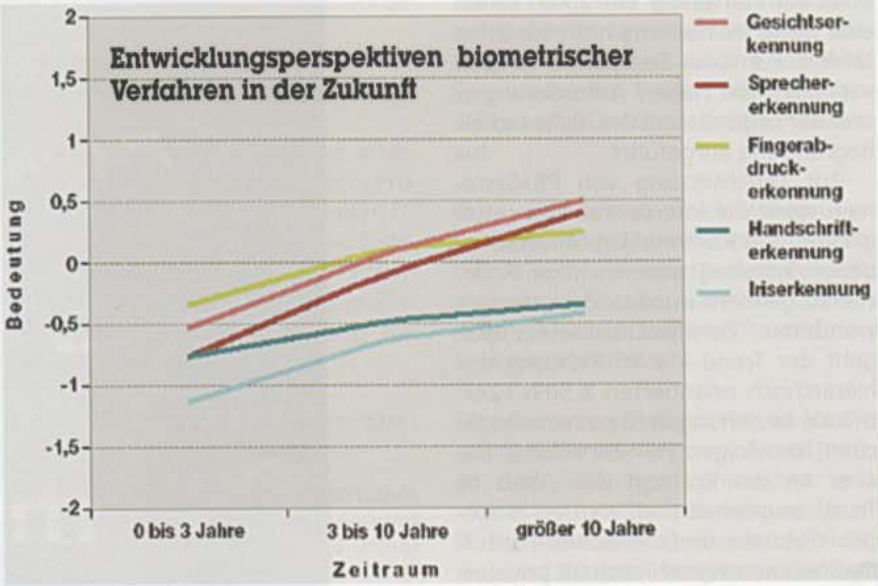
IuK-Sicherheit ökonomisch bedeutungslos?

Nach diesem Blick in die Zukunft der Technik lohnt es sich, die aktuelle Situation der IuK-Sicherheit aus einer ökonomischen Perspektive zu betrachten: In den letzten Jahren sind die Aufwendungen der Endnutzer für IuK-Sicherheit kontinuierlich gestiegen, in Westeuropa im Jahr 2002 auf stolze 9,4 Mrd. €. Das European Information Technology Observatory prognostiziert einen weiterhin starken Anstieg auf 12 Mrd. für 2003 und 18 Mrd. im Jahr 2005. Immerhin 3,7 Mrd. wurden im Jahr 2002 in Westeuropa für Sicherheitslösungen wie Firewalls, Anti-Viren-Software und Authentifizierungssysteme ausgegeben.

Viel Geld? Leider nein: Allein die beiden Viren „Code Red" und „Nimda" verursachten in 2002 weltweit einen geschätzten Schaden von 3,6 Mrd. €. Die aktenkundigen Sicherheitszwischenfälle in den großen Industriestaaten in den ersten neun Monaten desselben Jahres werden von der Carnegie Mellon University auf mehr als 73.000 beziffert. Und wenn man bedenkt, dass 2002 alleine die externen Ausgaben europäischer Unternehmen und Privatpersonen für IuK 594 Mrd. € betrugen, erscheinen die Gesamtausgaben für Sicherheit mit 9,4 Mrd. € bzw. 1,6% erschütternd bedeutungslos.

Trotz dieser ernüchternden Zahlen muss für Deutschland konstatiert werden, dass das Bewusstsein für die Notwendigkeit von IuK-Sicherheit hierzulande am ausgeprägtesten unter den großen europäischen Ländern ist. Der Einsatz von PKI beispielsweise ist in Deutschland im europäischen Vergleich am weitesten verbreitet. Aber: von den Beschäftigten öffentlicher Einrichtungen und Behörden wird IT-Sicherheit erst in 2008 als notwendig und sinnvoll angesehen, in den Unternehmen ist dies 2006 der Fall.

Die Hemmnisse für eine rasche Entwicklung des Marktes für IuK-Sicherheit sind hohe Preise für neue Technologien und der steigende Verwaltungs- und Einrichtungsaufwand für derartige Technologien und Prozesse. Noch weitaus häufiger werden als Argumente gegen eine Ausweitung der Sicherheitsvorkehrungen unerwünschte Einschränkungen in der Funktionalität, Performance und/oder Flexibilität der Systeme sowie nicht vorhandene Gefahren genannt. Diese Aussagen belegen eine traurige Wahrheit: Das Grundproblem ist das mangelnde Problembewusstsein der Menschen, ob als Beschäftigte in Unternehmen oder als private Nutzer. Es scheint, als könnte das Risikobewusstsein mit dem Tempo der technischen Entwicklung nicht Schritt halten. Zwar wird erwartet, dass in vier Jahren sicherheitsbezogene Produkteigenschaften ein Entscheidungskriterium beim Kauf privater IT sein werden, aber Einschränkungen der Funktionalität zur Gewährleistung von Sicherheitsfunktionen werden in den nächsten zehn Jahren nicht akzeptiert werden! Genauso wenig wie kostenpflichtige Anonymisierungsdienste im Internet. Kevin Mitnick, einst legendärer Hacker und nach fünf Jahren Gefängnis heute Leiter eines IT-Sicherheitsunternehmens, drückt das Problem pointiert aus: Unternehmen „verschwenden ihre Energie für ausgeklügelte Technologien und physische Abwehrmaßnahmen. Das schwächste Glied in der Kette haben sie dabei vernachlässigt: die Mitarbeiter". An dieser Stelle muss auch George Orwells gedacht werden, dessen Geburtstag sich in diesem Jahr zum hundertsten Mal jährt und der in „1984" das „Ende der Anonymität" (übrigens der Titel eines beachtenswerten Buches des BSI über so genannte Datenspuren bei Sprach- und Datenübertragungen) voraussagte. Dass wir es dem Big Brother durch Unwissenheit und Leichtfertigkeit so einfach machen würden, konnte Orwell natürlich nicht ahnen. ■



Grafik: Keil