Mitgliederzeitung des Berufsverbandes der Datenschutzbeauftragten e.V. (BvD)

2. Ausgabe, Juli 1998

· · · · · Editorial · · · · ·

Liebe Mitglieder,

die Sommerpause steht vor der Tür und wir hoffen, daß Sie die Mitgliederzeitung noch rechtzeitig erreicht, um Ihnen als Urlaubslektüre zu dienen. Wir blicken auf ein ereignisreiches erstes Halbjahr 1998 zurück. Vom 31. März 1998 bis zum 1. April 1998 wurde der Datenschutzkongreß 1998 im Ulmer Stadthaus veranstaltet. Die Veranstaltung wurde zu einem vollen Erfolg und hat allen (wie wir hoffen) viele Informationen geboten und Freude bereitet. Interessante Vorträge waren zu hören, Kontakte wurden geknüpft und langjährige Mitstreiter aus der Datenschutzszene konnten wieder einmal die Köpfe zusammenstecken. Der BvD hat anläßlich seiner Mitgliederversammlung einen neuen Vorstand gewählt.
Auch mit wichtigen Datenschutzthemen waren die letzten Monate gespickt. Heiß diskutiert wurden das neue BDSG (das ja nun definitiv in dieser Legislaturperiode nicht mehr kommen wird), die von der Bundesregierung (immer noch) angestrebte Kryptoregulierung, der Aufbau einer Gendatei im Bundeskriminalamt, der Echelon-Skandal und viele andere Themen. Auch in dieser Ausgabe finden sich wieder einige Artikel, die aktuelle Probleme aufgreifen.
Eine wichtige und brandaktuelle Änderung beim BvD will ich Ihnen gleich an dieser Stelle mitteilen:
Da in der Vergangenheit öfters Probleme mit der Erreichbarkeit des BvD auftraten, versuchen wir schon seit längerer Zeit eine neue Geschäftsstelle zu etablieren. Dies gestaltete sich aufgrund unseres äußerst knappen Budgets sehr schwierig. Die angestrebte Zusammenarbeit mit der Ulmer Akademie für Datenschutz und IT-Sicherheit (wir berichteten) kam leider noch nicht zustande. Deshalb haben wir eine andere Lösung gesucht und nun auch gefunden. Die Adresse der neuen Geschäftsstelle lautet ab sofort.

Berufsverband der Datenschutzbeauftragten e. V.
Ehingerstraße 19
89077 Ulm

Tel.: 0731/6026265
Fax.: 0731/9608511

Die Webseiten und die E-Mailadressen bleiben bis auf weiteres unverändert (siehe auch Impressum).

Ihr Markus Mix

· · · · · BvD-Kongreß 1998 · · · · ·

Kongreßbericht

Dr. Alwin Baumeister, Öffentlichkeitsreferent des BvD

Der Bundesverband der Datenschutzbeauftragten Deutschlands e.V. (BvD) führte vom 31. März 1998 bis zum 1. April 1998 seinen Datenschutzkongreß 1998 im Ulmer Stadthaus durch. Datenschützern und Datenschutzinteressierten wurde von hochkarätigen Referenten aus der Datenschutz- und IT-Sicherheitsszene, aus Behörden, Politik und Wirtschaft ein weitgefächertes, aktuelles und praxisnahes Themenspektrum angeboten.

Nach einführenden Begrüßungsworten des Bundesvorsitzenden des BvD, Prof. Dr. Gerhard Kongehl, des OB der Stadt Ulm Ivo Gönner, des Landesdatenschutzbeauftragen von Baden-Württemberg Herrn Schneider und des Rektors der FH Ulm Prof. Dr. Hentschel referierte Prof. Kongehl im Eröffnungsvortrag über den Datenschutzbeauftragten als Fossil der Zukunft? (siehe auch seinen Beitrag in diesem Heft). In seinem Vortrag zeigte Prof. Kongehl deutlich und eindrucksvoll die Diskrepanz zwischen der Entwicklung auf dem IT- und Datenverarbeitungssektor und der Entwicklung, oder besser gesagt dem Stillstand in der Entwicklung des Datenschutzes und der Datensicherheit auf. Eine schleichende Gefahr auf einer Ebenen, die für den Betroffenen nicht wahrnehmbar ist, droht die künftige Entwicklung von Freiheitsrechten zu beeinträchtigen sowie die Gewähr der Nachhaltigkeit einzuschränken. Er rief unter anderen vorallem die Datenschutzbeauftragten auf diese Persönlichkeitsrechte jetzt zu sichern.

In seinem Vortrag über Lauschangriff und Personenkontrolle ohne Anlaß stellte Prof. Stephan von der FH Villingen-Schwenningen die Frage: Kann der Staat Freiheit sichern, indem er sie beschränkt? In seinen Ausführungen wurde deutlich, daß die Polizei immer mehr Aufgaben und somit auch Rechte zugespielt bekommt, die ihr grundsätzlich nicht zugedacht waren. Er setzte sich kritisch mit den verdeckten Ermittlern, dem „Großen Lauschangriff“, der Rasterfahndung, der Straffreiheit für Europol, dem angeblichen Zuwachs der organisierten Kriminalität, uvm. auseinander. In seinem Fazit aber brachte er deutlich hervor, daß der Staat, indem er die Freiheit des Bürgers einschränkt, um sie zu schützen, den Teufel mit dem Beelzebub austreibt. Die Perspektiven seien fatal: Nicht mehr Sicherheit bei weniger Freiheit für die Bürger, sondern vielmehr weniger Sicherheit bei weniger Freiheit.

Dr. Helmut Garstka, der Berliner Datenschutzbeauftragte, referierte zum Thema „Multimedia — Datenschutz bei Tele- und Mediendiensten“. Er stellte klar heraus, daß vielen Nutzern von Online-Diensten die Tragweite des „Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdiensten (Informations- und Kommunikationsdienste-Gesetz)“ sowie des Staatsvertrages über Mediendienste (beide vom 1. August 1997) nicht klar ist. Klare Abgrenzungen beider Materien fallen schwer. Kompetenzkonflikte zwischen Bund und Ländern, sowie zwischen den Autonomieanforderungen von Rundfunkanstalten sind vorprogrammiert und werden die Anwendung der Gesetze sehr erschweren. Er resümierte,

daß der Gesetzgeber von Bund und Ländern sich mutig auf ein neues Terrain gewagt hat, die Konsequenzen aber noch nicht nachvollzogen hat.

Im letzen Vortrag des ersten Kongreßtages beantwortete Dr. Hannes Federrath, ein Mitarbeiter in der Arbeitsgruppe von Prof. Pfitzmann am Institut für Theoretische Informatik an der TU Dresden die Frage: „Steganographie — Doch ein leistungsfähiges Verschlüsselungsverfahren?“ Mit der Steganographie können geheime Nachrichten übermittelt werden, ohne daß deren Existenz für Außenstehende überhaupt nachweisbar ist. Die Diskussionen um ein Kryptoverbot führten zu einer verstärkten Beachtung der „Wissenschaft vom Verstecken von Nachrichten“. Dr. Federrath nahm in seinem Vortrag das Potential der Steganographie aus der Sicht des Nutzers kritisch unter die Lupe. Er zeigte, daß einige der öffentlich bekannten und im Internet verfügbaren Verfahren Schwächen aufweisen und wie diese zu beheben sind. Er faßte zusammen, daß paradoxer Weise gerade die Kryptodebatte dazu beiträgt, daß steganographische Verfahren schrittweise verbessert und damit immer sicherer werden. (siehe auch seinen Beitrag in diesem Heft)

Zum Abschluß des Tages fand die Mitgliederversammlung des BvD statt. Sie hatte neben konstruktiven Diskussionen um aktuelle Themen des Datenschutzes und der Stellung des BvD zu einzelnen Themen die Neuwahlen des Vorstand im BvD auf der Tagesordnung.

Zu Beginn des zweiten Kongreßtages stand das Thema „Novellierung des BDSG“ auf dem Kongreßplan. Dr. Thilo Weichert, Vorsitzender der Deutschen Vereinigung für den Datenschutz und stellvertretender Landesbeauftragter für den Datenschutz in Schleswig Holstein stellte den nur teilweise intern abgestimmten Entwurf der Bundesregierung dem Entwurf von Bündnis 90/Die Grünen gegenüber. Beide Entwürfe basieren auf dem bestehenden BDSG, wobei er dem Entwurf der Bundesregierung vorwirft, dem alten BDSG von 1990 zum Teil systemfremde Regelungen überzustülpen, ohne auch nur ansatzweise die rasanten Technikentwicklungen oder die Diskussionen über ein modernes Datenschutzrecht zur Kenntnis zu nehmen. Gesetzestechnische und begriffliche Ungereimtheiten paaren sich mit Praxisferne. Die Verabschiedung dieses Entwurfes würde vorallem eines bewirken, so Dr. Weichert, die Diskreditierung des Datenschutzes allgemein. Im Entwurf des Bündnis 90/Die Grünen seien dagegen die neuen europäischen Regelungen integriert, der private und öffentliche Bereich teilweise vereinheitlicht und zugleich sind die Erkenntnisse der modernen datenschutzrechlichen Diskussion und die neuen technischen Entwicklungen verarbeitet. Als Ergebnis diese Entwurfes sieht Dr. Weichert die Abkehr vom klassischen, bereichsspezifischen Datenschutz und die Hinwendung zum Grundrechtsschutz durch Verfahren, Suche nach technischen Lösungen und den Aufbau eines mehrschichtigen Schutzinstrumentes. Er bemängelt auch, daß beide Entwürfe nur wenig Realisierungschancen vor der Frist für den Abschluß der Novellierung im Oktober 1998 haben, wobei deren Diskussion aber von großer Bedeutung für eine baldige sachgerechte Novellierung des deutschen Datenschutzrechtes in der 14. Legislaturperiode des Deutschen Bundestages sei.

In einem fundierten Vortrag über Datenschutzstrafrecht zeigte Prof. Dr. U. Sieber von der Universität Würzburg auf, wo das Datenschutzstrafrecht in Gesetzestexten verankert ist und stellte klar heraus, das jeder Verstoß gegen das Datenschutzrecht auch datenschutzstrafrechtlich zu verfolgen ist. Er skizzierte allgemein einen strafrechtlichen Deliktaufbau mit Tatbestandsmäßigkeiten und speziellen datenschutzrechtlichen Einordnungsproblemen am Beispiel Outsourcing. Weiterhin gab er Hinweise für Strafverfahren, sowohl für den Anzeigenerstatter, als

auch den Zeugen und den Beschuldigten. Prof. Sieber verstand es in dieses sehr komplexe Thema klare Strukturen zu bringen, so daß es greifbar und anwendbar wurde.
Zum Abschluß der Tagung zeigte Holger Heimann vom Ingenieurbüro Heimann am praktischen Beispiel, daß auf Grund von unerkannten und nicht beachteten Internetrisiken jeder sein eigener Datenschutzbeauftragter sein muß. Herr Heimann zeigte auf wie man ohne die neuen, subtilen Angriffsmethoden auf die Computer von Internetnutzern oder auf die Anbieter von Internetdiensten mit äußerst einfachen Mitteln zugreifen könnte. Der Ansatz zu diesen Angriffen trägt der Tatsache Rechnung, daß die größten und fatalsten Sicherheitslücken durch Unwissenheit und Administrationsfehler des Nutzer selbst entstehen. Oft versteckt sich die Komplexität einer Technik hinter der vermeindlichen Leichtigkeit der Verfügbarkeit und Bedienung. Bei dem beschriebenen Angriff wurden Dial-In-Pools von Providern im Internet gescannt, wodurch es möglich war, gerade eingewählte Rechner zu erkennen und auf bestimmte Verletzlichkeiten zu untersuchen und somit dann den betroffenen Rechner bei einer erneuten Einwahl wiederzuerkennen und dann nach einer off-line-Auswertung der gesammelten Daten diesen Computer gezielt anzugreifen, um Daten zu sammeln, zu kopieren, zu manipulieren oder zu löschen. Die möglichen Opfer reflektieren den Querschnitt der Nutzer solcher Einwähldienste und sind nicht nur Privatpersonen, sondern beispielsweise auch Unternehmen, Behörden, Polizeidiensstellen, Anwaltskanzleien, Arztpraxen, Kliniken usw. mit einem oft hoch kritischen Datenbestand. Dieses Angriffsverfahren macht es unter bestimmten Umständen auch möglich, sogar Sicherheitsbarrieren wie z.B. teure Firewalls auszutricksen und Angriffe auf lokale Netze hinter dem betroffenen Computer durchzuführen oder vorzubereiten.
Mit diesem Vortrag ging ein Datenschutzkongreß zu Ende, bei dem großen Wert darauf gelegt wurde, alle aktuellen und brisanten Datenschutzthemen zu behandeln und besonders kritisch von Praktikern durchleuchten zu lassen.

Protokoll der Mitgliederversammlung vom 31. 3. 1998

Am abend des ersten Tages des diesjährigen BvD-Kongresses fand in Ulm die Mitgliederversammlung des BvD statt. Hier das Protokoll zu Ihrer Information.

Anwesend: 21 Mitglieder
Sitzungsleiter: Dr. Herb
18:00-20:30 Uhr

Tagesordnung:

1. Eröffnung durch den Vorsitzenden
2. Genehmigung der Tagesordnung
3. Feststellung der Beschlußfähigkeit
4. Rechenschaftsbericht durch den Vorsitzenden
5. Bericht über den Stand der Umsetzung der EU-Richtlinie neues BDSG
6. Satzungsänderungen
7. Bericht der Kassenprüfer
8. Entlastung des Vorstandes
9. Neuwahl des Vorstandes
10. Neuwahl der Kassenprüfer
11. Weitere Anträge
12. Verschiedenes

1. Eröffnung durch den Vorsitzenden

Der Vorsitzende eröffnet die Sitzung um 18:00 Uhr im Ulmer Stadthaus.

Er schlägt Dr. Herb als Sitzungsleiter vor. Die Versammlung stimmt zu (einstimmig)

2. Genehmigung der Tagesordnung

Nach einer Umstellung der Tagesordnungspunkte wird die Tagesordnung genehmigt.

3. Feststellung der Beschlußfähigkeit

Es sind 21 Mitglieder anwesend. Damit wird die Beschlußfähigkeit festgestellt.

4. Rechenschaftsbericht durch den Vorsitzenden

Der Vorsitzende berichtet über die Tätigkeit des Vorstandes seit den letzten Wahlen.

5. Bericht über den Stand der Umsetzung der EU-Richtlinie neues BDSG

Dr. Herb berichtet über den letzten Stand der Dinge.

6. Satzungsänderungen

Die vom Vorstand vorgeschlagenen Satzungsänderungen wurden einstimmig genehmigt.

7. Bericht der Kassenprüfer

Der Bericht wurde dem Vorstand schriftlich vorgelegt.
Ein Punkt führte zur Diskussion: Nach Auffassung der Kassenprüfer wurde eine Rechnung in Höhe von DM 600,- doppelt bezahlt. Die 600,- DM sind entweder zurückzufordern oder es ist eine korrekte Rechnung vorzulegen.
Die Kassenprüfer sind bei 3 Enthaltungen und ohne Gegenstimmen entlastet worden.

8. Entlastung des Vorstandes

Der Vorstand ist mit 12 Stimmen bei 9 Enthaltungen und ohne Gegenstimmen entlastet worden.

9. Neuwahl des Vorstandes

Auf Vorschlag des Vorstandes wurde beschlossen, daß der Vorstand gemäß der neuen Satzung, neben dem Vorsitzenden, dem Stellvertretenden Vorsitzenden, dem Finanzreferenten und dem Beisitzer auch die folgenden Positionen umfassen soll: Justitiar, Organisationsreferent, Sicherheitsreferent und Öffentlichkeitsrefrent. Öffentlichkeitsreferent und Stellvertretender Vorsitzender sollen zusammengefaßt werden.
Im einzelnen wurden gewählt:

- Vorsitzender: Prof. Dr. Gerhard Kongehl (19 Stimmen, 2 Enth., keine Gegenst.)
- Stellv. Vorsitzender: Markus Mix (19 Stimmen, 2 Enth., keine Gegenst.)
- Finanzreferent: Helmut Kaitz (14 Stimmen, 6 Enth., 1 Gegenst.)
- Beisitzer: Dr. Alwin Baumeister (20 Stimmen, 1 Enth., keine Gegenst.)
- Justitiar: Dr. Armin Herb (20 Stimmen, 1 Enth., keine Gegenst.)
- Organisationsreferent: Dieter Gusenbauer (20 Stimmen, 1 Enth., keine Gegenst.)
- Sicherheitsreferent: Dr. Hannes Federrath (17 Stimmen, 4 Enth., keine Gegenst.)

10. Neuwahl der Kassenprüfer

Als Kassenprüfer wurden Frau Barbara Stoeferle und Herr Bernd-Rainer Boschek bei je einer Enthaltung einstimmig wiedergewählt.

11. Weitere Anträge

Keine.

12. Verschiedenes

Herr Roland Schäfer hat einen Katalog über die möglichen Aufgaben eines Berufsverbandes erstellt, den er vorließt. Anschließend wird über Möglichkeiten, diese Vorschläge umzusetzen, diskutiert. (siehe auch seinen Beitrag in diesem Heft)

Ende der Sitzung: 20:30 Uhr

Prof. Dr. Gerhard Kongehl
Protokollführer

····· Thema: Vereinsarbeit ·····

(Mögliche) Aufgaben eines Berufsverbandes

Roland Schäfer, Mitglied des BvD

Nicht nur auf der Mitgliederversammlung des BvD am 31. 3. 98 gab es Diskussionen um die Aufgaben eines Berufsverbandes. Der folgende Beitrag greift verschiedene Punkte auf und soll zur Diskussion auch innerhalb der Mitglieder des BvD anregen.

1. Die Erreichbarkeit des BvD muß gewährleistet sein.

D. h., es genügt nicht, daß ein automatischer Anrufbeantworter unter einer „Hotline Nummer" Nachrichten weiterleitet, sondern ein Mensch muß die Weiterleitung zusagen können (Sekretariat). Besser noch, ein [Wort fehlt, Anm. d. R.] stiftet Kontakte zwischen den Vereinsmitgliedern (Geschäftsführer).

2. Der BvD braucht eine regionale und fachliche Struktur, die (wenigstens) den Berufsverbandsmitgliedern bekannt ist.

Ziel ist es, daß der erste Ansprechpartner für Mitglieder und Nichtmitglieder weniger als 100 km entfernt ist (Landesverbände).

Ferner ist es Ziel, daß bekannt wird, wer sich fachlich intensiver mit Einzelthemen beschäftigt (hat), z.B. Datenschutz in der Mobiltelefonie, betrieblicher Datenschutz beim SAP System, etc. (bundesweite Fachausschüsse). Schließlich sollten die Cracks zu Einzelthemen – EDV oder juristischen – bekannt sein, damit die bDSBen aus einem Pool von Sachverstand für ihre Aufgaben schöpfen können (Sachverständigen Pool).

3. Der BvD braucht ein Informations-, Material- und Literaturaustausch.

Zum Teil wird dies über die „Mitgliederinformationen" bereits erfüllt.

- Auf welche Informationsquellen kann ein Mitglied zurückgreifen?
- Welche Materialien stehen zur Verfügung?
- Gibt es eine Bibliothek zum Datenschutz (in meiner Nähe)? Z.B. ist die GDD Studie „Datenschutz in Deutschland" für das einzelne Mitglied zu teuer, der Verband könnte sich ein Exemplar leisten.

Läßt sich in diesem Zusammenhang die Zusammenarbeit mit der Redaktion der Zeitschrift DuD intensivieren?

4. Der BvD braucht Foren zum einfachen Erfahrungsaustausch.

Es genügt nicht, daß ein 4 bis 12 köpfiges Gremium in Ulm sich Gedanken zu den Problemen der bDSBen macht. In diese Diskussion müssen mit vertretbaren Aufwänden alle Mitglieder einbezogen sein (Landesverbände, bundesweite Fachausschüsse).

5. Der BvD muß heikle Themen angehen und Handlungshilfen den bDSBen geben.

Solche heiklen Themen sind:

- Verstößt der BDSB in seiner Beratungspraxis gegen das Rechtsberatungsgesetz?
- Wie ist er vor einem Bußgeldverfahren geschützt?
- Wie kann ein BDSB berufsbegleitende Qualifizierungsmaßnahmen fordern und rechtfertigen, ohne sich ein Blöße in seiner „Fachkunde" zu geben?

6. Der BvD braucht Diskussionsforen zu einzelnen Themen.
Er braucht – in der Regel – nicht die Vorstandsmeinung zu diesen Themen.
Themenbeispiele:

- Vereinbarkeit des Amtes als Betriebs- oder Personalrats einerseits und des Amtes als BDSB andererseits,
- Kontrolle des BDSB gegenüber dem BR/PR und umgekehrt,
- Externe bDSBe und (fehlende) Betriebskenntnisse,
- Datenschutz in den Tele- und Mediendiensten,
- Datenschutz Audit.

Roland Schäfer, Fachkraft für Datenschutz, Frankfurt am Main, Ruf 069 - 565 414, Fax 069 - 565 415, datenschutz.schaefer@t-online.de

Ulm, am Dienstag, den 31. März 1998

Einbeziehung der Mitglieder in die Verbandstätigkeit

ein Aufruf von Markus Mix

Regionalgruppe Großraum Rhein-Main
Herr Roland Schäfer (siehe auch seinen obigen Beitrag in diesem Heft) bietet an, die Gründung einer **Regionalgruppe Großraum Rhein-Main** (Plz: 60*, 61*, 63*, 65* und 35*) zu moderieren. Mitglieder, die an regionaler Zusammenarbeit und Erfahrungsaustausch interessiert sind, möchten sich bitte bei ihm melden:
Roland Schäfer
Fachkraft für Datenschutz
Flensburger Straße 22
60435 Frankfurt am Main
Ruf: +49 (0) 69 - 565 415
Fax: +49 (0) 69 - 565 415
Mobil: +49 (0) 172 - 68 20 30 8
e-mail: datenschutz.schaefer@t-online.de

Vorhandene Regionalgruppen
In der Vergangenheit haben sich verschiedene Regionalgruppen und Arbeitskreise unter den Mitgliedern gebildet. Welche ist noch aktiv? Bitte melden Sie sich bei der Geschäftsstelle, wenn Sie noch regelmäßige Treffen oder andere Aktivitäten veranstalten. Sehr freundlich wäre es, wenn Sie uns eine Anlaufstelle nennen könnten, die wir dann in der nächsten Mitgliederzeitung und in den Informationsbroschüren für neue Mitglieder veröffentlichen können. Vielleicht ist ja jemand aus Ihrer Region an einer Mitarbeit interessiert und hat nur keinen Ansprechpartner...

Verbesserung der Außenwirkung des BvD
Um die Außenwirkung des BvD überregional zu verbessern, wollen wir in Zukunft bundesweit in regionalen Tageszeitungen durch Presseerklärungen auf die Belange des Datenschutzes aufmerksam machen.
Wir möchten versuchen, einen BvD-Presseverteiler unter den Mitgliedern zu etablieren. Pressemitteilungen, die vom BvD herausgegeben werden, sollen auf diese Weise auch in regionalen Tageszeitungen erscheinen. Wir suchen Mitglieder, die sich bereiterklären, Pressemitteilungen an die lokale Presse, am besten direkt an einen verantwortlichen Redakteur, weiterzugeben. Wenn Sie eine Möglichkeit sehen, Presseerklärungen in Ihrer Lokalzeitung unterzubringen, melden Sie sich bitte bei der Geschäftsstelle, um die Details zu besprechen.

Vorstellung des neuen Vorstandes

Den beiden nachfolgenden Tabellen können Sie die Mitglieder des Vorstandes und der weiteren Funktionsträger, ihre Aufgaben und die Beratungsangebote für Mitglieder entnehmen.

Die Funktion des Webmasters ist zur Zeit unbesetzt. Wer sich kompetent fühlt, diese Aufgabe zu übernehmen, ist eingeladen, aktiv mitzumachen.

Vorstand des BvD

Funktion im Vorstand	Person	E-Mail	Aufgaben
Vorsitzender	Prof. Dr. Gerhard Kongehl	Ulmprivacy@aol.com, Kongehl@fh-ulm.de	Pressemitteilungen, Kolumne „Der Datenschutzskandal des Monats“, Außen- und Medienvertretung, Mitgliederberatung in politischen- und Praxisfragen zum Datenschutz
Stellv. Vorsitzender	Markus Mix	M.Mix@von.ulm.de	Mitgliederzeitung Mitgliederberatung in Fragen zur IT-Sicherheit
Sicherheitsreferent	Dr. Hannes Federrath	federrath@inf.tu-dresden.de	Mitgliederberatung in Fragen zur IT-Sicherheit
Justitiar	Dr. Armin Herb	Nur Fax: 0711-929-3019	Justitiar, Führung des Lobbyverzeichnisses beim Bundestag, Mitgliederberatung in Rechtsfragen
Organisationsreferent	Dieter Gusenbauer	gusenbauer@t-online.de	Organisation Vorstandssitzungen, Protokollführung, Anträge DuD zum halben Preis, Mitgliederverwaltung
Finanzreferent	Helmut Kaitz	Helmut_Kaitz@peoplesoft.com	Finanzen
Beisitzer	Dr. Alwin Baumeister	Alwin.Baumeister@aai.de	DuD-Kolumne

Weitere Funktionen/Verantwortlichkeiten im BvD

Funktion	Person	E-Mail
Geschäftsstelle	Martina Mix	M.Mix@von.ulm.de
Kassenprüfer	Barbara Stoeferle, Bernd-Rainer Boschek	
Webmaster	n.n.	
Steuerberaterin	Frau Kaitz	

Die Vorträge auf dem BvD-Kongreß
····· Teil 1 ·····

Der Datenschutzbeauftragte — Fossil der Zukunft?

Gerhard Kongehl

Die Zeiten, als der maschinenlesbare Personalausweis oder die Volkszählung von 1987 die Datenschützer und ihre Sympathisanten zu Proteststürmen anfachten, kommen uns heute schon recht idyllisch vor. Die Gefahren der Technik für die Privatsphäre des Bürgers sind inzwischen ja von weit größerem Kaliber. Eigentlich müßten dies Zeiten der Hochkonjunktur für uns Datenschützer sein. Jedoch die Verhältnisse, sie sind nicht so. Man regt sich über den scheibchenweisen Verlust der Privatsphäre meist nur dann noch auf, wenn man selbst betroffen ist. Diese Betroffenheit ist durchaus im doppelten Sinne zu sehen: Entweder weil einem tatsächlich Stück persönlicher Freiheit abhanden zu kommen droht, aber auch, weil man von der Betroffenheit anderer (zum Beispiel als Journalist, aber natürlich auch als Datenschützer) profitieren kann.

Es sind aber nicht nur die zunehmenden Überwachungsmöglichkeiten des Staates und die Auswertungsmöglichkeiten von Datenspuren des Individuums durch die Wirtschaft, die den Datenschutz langsam aber stetig an den Rand der Gesellschaft drängen. Es liegt auch an der Duldungsstarre dieser Gesellschaft, die für einen vermeindlichen momentanen wirtschaftlichen Vorteil eine zunehmende und langfristig sich verheerend auswirkende Verluderung des Datenschutzes in Kauf nimmt.

So sind zwar seit nunmehr 20 Jahren in der Bundesrepublik Deutschland die meisten Unternehmen (und immer mehr öffentliche Stellen) verpflichtet, einen Beauftragten für den Datenschutz zu bestellen, aber immer noch kommen viele Institutionen dieser gesetzliche Pflicht entweder überhaupt nicht nach oder sie interpretieren die vom BDSG leider sehr unverbindlich gehaltenen Forderungen der Fachkunde und Zuverlässigkeit des Datenschutzbeauftragte ausschließlich in Sinne eigener wirtschaftlicher Überlegungen.

Nach der gegenwärtigen Rechtslage läßt das BDSG sowohl einen internen (also in der Regel angestellten) als auch einen externen (freiberuflichen) Datenschutzbeauftragte zu. Wann welche Art von Datenschutzbeauftragten sinnvoll ist, sagt das Gesetz nicht. Wenn man die Vor- und Nachteile der beiden Arten von Datenschutzbeauftragten gegeneinander abwägt, zeigt sich, daß der fachkundige, mit einem ausreichenden Zeitbudget ausgestattete interne Datenschutzbeauftragte die bessere Lösung ist. Es sind vor allem die folgenden Aspekte, die der interne in die Waagschale werfen kann:

- Permanente Präsenz in Betrieb/Behörde.
- Kündigungsschutz, daher weisungsfrei tätig.
- Unabhängig im Sinne der Datenschutz-Richtlinie der EU.
- Kompromißbereitschaft nur im Sinne der Sache, nicht wegen wirtschaftlicher Abhängigkeit.
- Gute Kenntnisse in der innerbetrieblichen Organisation, da Teil davon.

- Konzentriert seine Tätigkeit auf eine einzige Institution.
- Kein persönlicher Profit des Datenschutzbeauftragten bei geringerem Zeiteinsatz, bei mangelnder Fortbildung und bei der Verlagerung der Tätigkeit auf Hilfskräfte.
- Macht viel selbst und tut dies fachkundig, da weniger Möglichkeiten der Verlagerung von Tätigkeiten auf geringer qualifizierte Hilfskräfte.
- Mitarbeiter des Datenschutzbeauftragten unterliegen der Mitbestimmung des Betriebs- bzw. Personalrats.
- Bei größeren Institutionen in der Regel kostengünstiger (!) als ein Externer bei gleichem Zeiteinsatz (siehe Unikliniken in Baden-Württemberg).

Lediglich bei kleinen Institutionen wird das Kosten-Nutzen-Verhältnis zu ungünstig, so daß der externe Datenschutzbeauftragte auch aus Gründen des Datenschutzes akzeptabel erscheint.

Im Augenblick geht die Entwicklung gerade in die falsche Richtung: Ob man einen internen oder externen Mitarbeiter zum Datenschutzbeauftragten bestellt, wird anhand von wirtschaftlichen Kriterien (zu denen auch die einfache Möglichkeit der Kündigung des Externen zu zählen ist) und nicht von den Erfordernissen des Datenschutzes her entschieden. Größere Unternehmen (z.B. Kliniken) neigen immer mehr zum leichter zu beeinflussenden externen Datenschutzbeauftragten, kleine Unternehmen (z. B. Arztpraxen) wollen – wenn überhaupt – eher einen internen, der natürlich vor allem eine Alibifunktion zu erfüllen hat.

Wenn die Datenschutzbeauftragten auch in Zukunft einen ansehnlichen Beitrag zur Wahrung des informationellen Selbstbestimmungsrechts des Bürgers leisten und nicht zum Fossil der Steinzeit der Informationsgesellschaft degenerieren sollen, dann muß solchen Fehlentwicklungen Einhalt geboten werden. Dazu muß zunächst einmal die Tätigkeit der Datenschutzbeauftragten auf eine bessere rechtliche Grundlage gestellt werden.

Verbesserung heißt hier auch, daß verschiedene Sachverhalte genauer definiert werden müssen. Das gilt für die Fachkunde ebenso wie für die Zuverlässigkeit. In neuen gesetzlichen Regelungen muß darüber hinaus unbedingt zwischen der Tätigkeit eines internen und einem externen Datenschutzbeauftragten unterschieden und festgelegt werden, wann der eine und wann der andere tätig werden soll. Auch muß es für den Externen eine Begrenzung bei der Zahl der zu betreuenden Unternehmen bzw. Behörden geben. Der BvD wird in Kürze entsprechende Vorschläge im Zusammenhang mit der beabsichtigten Novellierung des BDSG vorlegen.

Die Abwehrmechanismen bei Unternehmen und Behörden in bezug auf den Datenschutz basieren aber nicht nur auf Wirtschaftlichkeitsüberlegungen. Sie liegen auch daran, daß man vom Datenschutz keinen sinnvollen Beitrag zur Technikgestaltung erwartet. Im Gegenteil, in vielen Institutionen empfindet man den Datenschutz sogar als Hindernis bei der Problemlösung und der Aufgabenerfüllung. Deshalb werden auch die Datenschutzbeauftragten vielerorts wie lästige Fahrkartenkontrolleure der Eisenbahn betrachtet, die zwar die Beförderungsbedingungen der Bahn sicherstellen können, jedoch keinen Einfluß darauf haben, daß der Zug seine Fahrgäste pünktlich zum gewünschten Zielbahnhof befördert. Oder wie es Lutterbeck in DuD 3/98 sagte: Sie schaffen Leitplanken für nicht existierende Autobahnen an.

Wer von unseren Berufskollegen tatsächlich die vom Gesetz vorgeschriebenen Melde- und Dokumentationspflichten in den Mittelpunkt seiner Arbeit stellt, wem es Erfüllung seines Lebenstraums bedeutet, als „Schriftgelehrter“ Datenschutz-Vorschriften in Form von Datenschutz-Statuten, Datenträger-Verordnungen, Paßwort-Empfehlungen, und Fax-Richtlinien umzusetzen, der darf sich

nicht wundern, wenn er — um noch mal Lutterbeck zu zitieren, als Datenschützer in der staubigen Ecke steht, während um ihn herum eine friedliche Revolution stattfindet. Diese Bürokratisierung des Datenschutzes ist es, die dem Datenschutz seine Akzeptanzprobleme schafft. Anscheinend werden aber diejenigen unserer Kolleginnen und Kollegen, die die Technikgestaltung, die problemorientierte Beratung und die Bewußtseinsbildung in den Mittelpunkt ihrer Arbeit stellen, in der Öffentlichkeit nicht genügend wahrgenommen. Das wiederum mag auch daran liegen, daß es zwar ein Berufsbild des Datenschutzbeauftragten (z.B. im „Ulmer Urteil“ vom 31. 10. 1990; Az: 5T 153/90-01 LG Ulm) aber keine einheitliche Berufsausbildung auf der Basis von – im Unterschied zu §37 BDSG – zeitgemäßen Aufgabenbeschreibungen gibt.

Auch die Ausbildung von Datenschutzbeauftragten nach dem Ulmer Modell, die die Fachhochschule Ulm - Hochschule für Technik seit 1987 anbietet, kann nur ein Zwischenschritt sein, ein Modell für die neunziger Jahre. Im nächsten Jahrzehnt müßte sie zu einem eigenständigen Studium weiterentwickelt werden.

Vorstellbar wäre ein achtsemestriges Studium an einer Fachhochschule zum diplomierten IT-Sicherheitsingenieur, in welchem zu gleichen Teilen Datenschutz und IT-Sicherheit gelehrt würde. Schwerpunkte dieser Ausbildung müßten u.a. sein:

- Grundlagen der Informatik
- Informatik und Gesellschaft/Datenschutz
- Recht
- Organisation
- IT-Sicherheit
- Datenschutzfreundliche Technik
- WISO-Fächer
- Praktische Tätigkeit
- Diplomarbeit

Ein solches Studium bzw. Diplom könnte dann die Voraussetzung für die Bestellung zum Datenschutzbeauftragte sein. Natürlich bedarf es in diesem Zusammenhang gründlicher Überlegungen zu Übergangsregelungen und zu Weiterbildungsangeboten für die bisher praktizierenden Datenschützer.

Steganographie – doch ein leistungsfähiges Verschlüsselungsverfahren?

Hannes Federrath

Mit Steganographie können geheime Nachrichten über offene, unsichere Datennetze übermittelt werden, ohne daß deren Existenz für Außenstehende überhaupt nachweisbar ist. Die Diskussionen um ein Kryptoverbot führten zu einer verstärkten Beachtung der „Wissenschaft vom Verstecken von Nachrichten“.

1. Einführung

Seit etwa 3 Jahren entwickelt sich verstärkt ein neues Forschungsgebiet, das sich insbesondere dem *Verbergen von Information* vor Angreifern in Rechnernetzen verschrieben hat (Information Hiding). Der klassische Fall des Information Hiding ist das Verschlüsseln von Nachrichten zum Zwecke der Geheimhaltung vor Außenstehenden. Neben der wohl ältesten Teildisziplin, der Kryptographie, aus der das neue Forschungsgebiet auch hervorgegangen ist, werden nun verstärkt Methoden zum

1. Verbergen von Nachrichten selbst sowie
2. Verbergen von Kommunikationsbeziehungen zwischen Teilnehmern in Kommunikationsnetzen und hier insbesondere Verbergen von

– Protokolldaten,
– Abrechnungsdaten,
– Aufenthaltsorten etc.

untersucht. Die Basistechnologien des Information Hiding sind

- Kryptographie,
- Steganographie,
- Spread Spectrum Technologien und
- (Kommunikations)-Protokolle zum Verbergen von Informationen.

2. Grundsätzliches zur Steganographie

Mit Steganographie wird eine geheimzuhaltende Nachricht in eine Hülle derart eingebettet, daß im Ergebnis

1. die minimalen Veränderungen der Hülle kaum bzw. nicht erkennbar sind und
2. die Veränderungen nicht mit Meßmethoden nachweisbar sind.

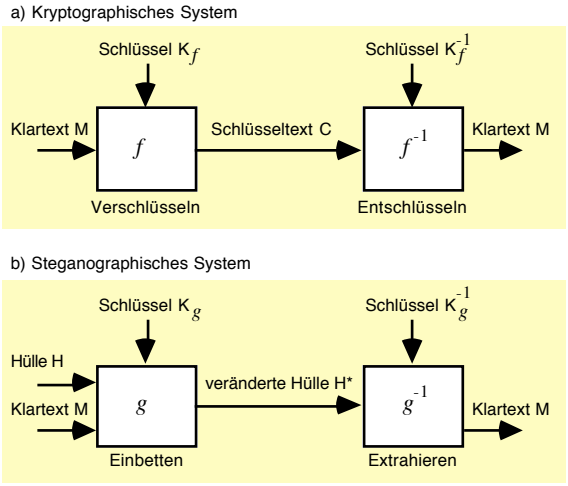

Abbildung 1: Grundaufbau von kryptographischem und steganographischem System

Als Hülle kann jedes Medium dienen, das einen indeterministischen Prozeß, z.B. eine Quantisierung, durchlaufen hat. Digitalisierte Sprache oder Musik, digitalisierte Bilder, Videos etc. sind hervorragend als Medien geeignet. Im Computer künstlich erzeugte Grafiken sind beispielsweise nicht gut geeignet. Steganographie ist technisch gesehen *keine* Verschlüsselung von Daten. Abbildung 1 soll dies deutlich machen.

Während bei Kryptographie der Klartext M mittels einer kryptographischen Funktion f in einen für jeden Außenstehenden, d.h. jeden, der nicht den Schlüssel K_f besitzt, unleserlichen Schlüsseltext C überführt wird, entsteht bei Steganographie als Ergebnis der Einbettungsfunktion g eine veränderte Hülle H^*, die für jeden Außenstehenden, d.h. jeden, der nicht den Schlüssel K_g besitzt, ebenso eine unveränderte Hülle H hätte sein können. Auf den Punkt gebracht bedeutet dies, daß die Verwendung von Verschlüsselung für den Außenstehenden zumindest erkennbar ist. Obwohl er nicht in Kenntnis des Nachrichteninhalts kommt, entsteht zumindest der Verdacht, daß die Kommunikationspartner etwas zu verbergen haben. Die Steganographie geht hier einen anderen Weg und kann damit die Existenz einer geheimen Botschaft verbergen. In einer offenen, unverfänglichen und unverschlüsselten Kommunikation wird unbemerkt eine geheime Botschaft transportiert. Das Grundprinzip der Steganographie setzt keine vorherige Verschlüsselung der geheimen Botschaft voraus, obgleich sie der Geheimhaltung auch nicht schadet.

Unabhängig von der Güte existierender steganographischer Systeme, auf die im nächsten Abschnitt eingegangen wird, müssen bei der Verwendung von Steganographie folgende Randbedingungen eingehalten werden:

1. Das (digitale) Original einer Hülle muß nach der erfolgten Einbettung unwiederbringlich vernichtet werden. Durch einen einfachen Vergleich des Originals mit der veränderten Hülle H^* wäre sonst ein Aufdecken der geheimen Kommunikation möglich.
2. Aus 1. folgt auch: Eine Hülle darf nie mehrmals verwendet werden, um unterschiedliche geheime Botschaften zu transportieren.

3. Brechen steganographischer Systeme

Das Brechen steganographischer Systeme ist zweistufig (vgl. [ZFPW_97]):

- Stufe 1: Erkennen, daß etwas eingebettet wurde. Dies bedeutet noch nicht, daß die geheime Botschaft offengelegt wurde. Dies erfolgt erst in Schritt 2:
- Stufe 2: Offenlegen der Botschaft.

Ein steganographisches System, das gemäß der Stufe 1 gebrochen wurde, ist unnütz und erfüllt seinen Zweck nicht. Will man sich lediglich sichern gegen ein Brechen der Stufe 2, ist die Wahl eines kryptographischen Verschlüsselungssystems angebracht, da es seine Aufgabe effizient erfüllt und kryptographische Systeme weitaus besser untersucht sind als steganographische.

Gute steganographische Systeme zeichnen sich mindestens durch folgende Eigenschaften aus:

- Algorithmus ist vollständig offengelegt.
- Es erfolgt eine Parametrisierung durch einen steganographischen Schlüssel.
- Die Einbettung beruht auf indeterministischen Effekten natürlichen Ursprungs (z.B. Quantisierungsrauschen, natürliche Störungen etc.)

Leider existiert bisher kein Beweis der Sicherheit eines Systems. Es läßt sich jedoch zeigen, daß unter bestimmten Umständen informationstheoretisch sichere Steganographie möglich ist (vgl. [KIPi_97]).

In [West_97] wurden einige Untersuchungen zur Güte existierender, frei (im Internet) verfügbarer steganographischer Systeme vorgenommen. Es zeigte sich, daß die Systeme meist schlecht sind, d.h. einfach gebrochen werden können. Das Wissen über die Sicherheitslücke führt in vielen Fällen zu deren unmittelbarer Beseitigung. Am Beispiel des Algorithmus Jsteg soll dies deutlich gemacht werden.

4. Brechen und Verbessern von Jsteg

Jsteg ist im Internet beispielsweise unter ftp://ftp.funet.fi/pub/crypt/steganography/ zu finden. Der Algorithmus von Jsteg basiert auf der weit verbreiteten Jpeg-Kompression. Die verlustbehaftete Kompression nach dem Jpeg-Verfahren ist besonders geeignet für Bildinformation mit fließenden Helligkeits- und Farbübergängen, z.B. digitale (oder digitalisierte) Fotografien. Sie beruht auf der diskreten Kosinustransformation (DCT) und zerlegt ein Pixelbild in einzelne Bildblöcke, meist aus 8x8 Pixeln bestehend, die dann in sog. DCT-Koeffizienten transformiert werden. Ein Koeffizient in einem Jpeg-Datenstrom repräsentiert einen Anteil am Farb- bzw. Helligkeitsverlauf im betrachteten Bildblock.

Das Einbetten bei Jsteg beruht auf dem einfachen Überschreiben von Informationsbits der DCT-Koeffizienten mit einer sehr geringen Bedeutung für den visuellen Eindruck, d.h. einfaches Ersetzen durch die geheime Botschaft.

Es wurden folgende Angriffe durchgeführt:

1. Visuelle Analyse, d.h. sehr genaues Betrachten verschiedener Bilder, Berechnen von Histogrammen über Farbverteilung, Helligkeit etc. Die durchgeführten Analysen lieferten keine Anhaltspunkte.

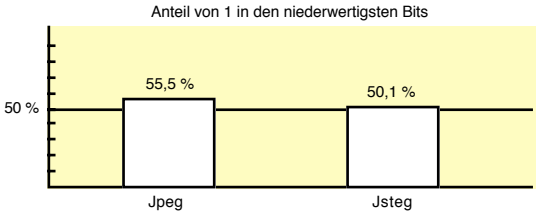

Abbildung 2: Häufigkeitsverteilung der niederwertigsten Bits

2. Häufigkeitsverteilung der niederwertigsten Bits. Es zeigte sich, daß in einem reinen Jpeg-Datenstrom, also ohne Steganographie, ein leichtes Übergewicht von Einsen in den niederwertigsten Bits zu finden ist. Folglich müßte beim Einbetten, d.h. beim Überschreiben der niederwertigsten Bits, darauf geachtet werden, daß die Häufigkeiten von Einsen und Nullen erhalten bleiben. Die Steganographie nach

Jsteg beachtet diesen Sachverhalt jedoch nicht, was zur Folge hat, daß beispielsweise bei der Einbettung einer zur Erhöhung der Sicherheit bereits (vor)-verschlüsselten Nachricht sich die Häufigkeiten von Null und Eins ausgleichen (siehe auch Abbildung 2).

3. „Treppenangriff". Bei diesem Angriff werden nun nicht nur die niederwertigsten Bits, sondern die DCT-Koeffizienten als Ganzes betrachtet. Bei einem normalen Jpeg-Bild zeigt sich eine typische Häufigkeitsverteilung der DCT-Koeffizienten, die in Abbildung 3a dargestellt ist. Berechnet man nun die Häufigkeitsverteilung für ein mit dem Jsteg-Algorithmus verändertes Bild, zeigt sich ebenfalls ein typischer Verlauf, der jedoch erheblich von dem bei Jpeg abweicht (Abbildung 3b). Dies deckt die Verwendung des Jsteg-Algorithmus auf, führt jedoch nicht unmittelbar zum Aufdecken der geheimen Botschaft. Der Grund für die auffällige Veränderung der Häufigkeitsverteilung liegt im Ausgleich der Häufigkeiten benachbarter Koeffizienten, bedingt durch das einfache Überschreiben ohne Beachtung der höherwertigen Bits. Die Kenntnis dieses Angriffs führt unmittelbar zu einer leichten Modifikation des Jsteg-Algorithmus: Ist das niederwertigste Bit eines Koeffizienten zu ändern, wird beispielsweise der gesamte Koeffizient um 1 reduziert.

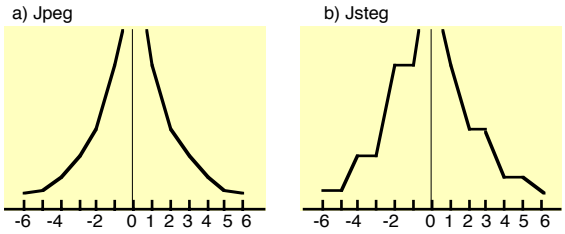

Abbildung 3: Häufigkeitsverteilungen der DCT-Koeffizienten

Der beschriebene Treppenangriff ist nicht nur auf Jsteg anwendbar, sondern auf alle steganographischen Algorithmen, die lediglich das niederwertigste Bit überschreiben.

5. Fazit

Die Darstellungen zeigen, daß die „Wissenschaft vom Verstecken von Nachrichten" (Steganographie) gerade begonnen hat, sich ernsthaft und kritisch mit ursprünglich spielerisch und ad hoc entstandenen Verfahren auseinanderzusetzen. Die „kritische Masse" war vor etwa 2 bis 3 Jahren erreicht, als in der Politik ernsthaft ein Kryptoverbot bzw. eine Reglementierung von Kryptographie diskutiert wurde. Hinzu kam und kommt die zunehmende Bedeutung von Multimedia und der damit verbundene Wunsch, auch die Urheberrechte bei der Verbreitung digitaler Objekte (Daten, Programme, Computerkunst etc.) über CD-ROM und Internet zu sichern. Die hierzu verwendeten technischen Mechanismen des Watermarking und Fingerprinting sind der Steganographie sehr ähnlich. Es ist zu erwarten, daß die Weiterentwicklung von Watermarking und Fingerprinting auch Folgen für die Verbesserung steganographischer Systeme haben wird.

6. Literatur

KlPi_97 Herbert Klimant, Rudi Piotraschke: Informationstheoretische Bewertung steganographischer Konzelationssysteme. Proc. Verläßliche IT-Systeme (VIS'97), DuD Fachbeiträge, Vieweg 1997, 225-232.

West_97 Andreas Westfeld: Steganographie in komprimierten Videosignalen. Diplomarbeit, TU Dresden, Institut für Theoretische Informatik, Juli 1997.

ZFPW_97 Jan Zöllner, Hannes Federrath, Andreas Pfitzmann, Andreas Westfeld, Guntram Wicke, Gritta Wolf: Über die Modellierung steganographischer Systeme. Proc. Verläßliche IT-Systeme (VIS'97), DuD Fachbeiträge, Vieweg 1997, 211-223.

····· Presseschau ·····

Pressestimmen über die Aktivitäten des BvD

Auch diesmal gab es wieder einige Pressemeldungen — vor allem Reaktionen auf den BvD-Kongreß.

Wie sicher sind unsere Daten?

Prof. Dr. Gerhard Kongehl, Vorsitzender des Berufsverbands der Datenschutzbeauftragten, Fachhochschule Ulm, über Späher im Internet

SZ: *Bei Ihrer Jahrestagung vergangene Woche in Ulm haben Sie festgestellt, daß viele Rechner nicht ausreichend vor Hackern geschützt sind. Zudem haben nun schon wieder Jugendliche die neue, angeblich verbesserte Software von T-Online geknackt. Müssen wir befürchten, daß die Daten von Firmen, Behörden und sogar die auf unseren privaten Rechnern nicht sicher sind?*
Kongehl: Das hängt ganz davon ab, welche Sicherheitsvorkehrungen getroffen worden sind. Aber viele vergessen, daß sich hinter den bunten Bildern auf dem Bildschirm eine zweite nicht sichtbare Ebene verbirgt, wo sich die Angreifer tummeln. Wer im Internet surft, vergißt häufig, daß die Telephonleitung keine Einbahnstraße ist.
SZ: *Welches Ergebnis hat Ihr Test erbracht?*
Kongehl: Zwischen zwölf und dreizehn Prozent der Computer waren nicht ausreichend gesichert.
SZ: *Was empfehlen Sie?*
Kongehl: Firewalls, also Brandschutzmauern, von denen heute alle reden, sind das gängige Rezept, um sich vor unerwünschen Besuchern zu schützen. Das ist allerdings auch ein Trugschluß, denn wenn man sich eine Firewall anschafft, dann bedeutet das noch lange nicht Sicherheit. Eine Firewall muß gut verwaltet werden, und man muß ständig überwachen, ob sich nicht Angreifer an der Firewall zu schaffen machen. Außerdem nutzt die beste Firewall nichts, wenn Firmen ein paar Privilegierten erlauben, sich per Modem von außen in das Netz einzuwählen und die Firewall zu umgehen. Wer ein Modem betreibt, obwohl es verboten ist, dem muß man mit Kündigung drohen, weil er auf diese Weise die gesamte Sicherheit aushebelt.

„Die Telephonleitung ist keine Einbahnstraße"

SZ: *Es gibt also Hintertüren...*
Kongehl:...Hintertüren, die nicht geschlossen sind. Hinzu kommt, daß viele Firmen chaotisch gewachsene Rechner-Netze betreiben, die nicht mehr überschaubar sind. All dies ist freilich keine Entschuldigung, nicht in die Sicherheit zu investieren. Bei uns an der Fachhochschule Ulm lernen die Studenten etwa, wie man Sicherheitskonzepte entwirft.
SZ: *Was empfehlen Sie Privatleuten?*
Kongehl: Das Wichtigste ist, daß man von sich aus Sicherheit plant. Mit dem Surfen entstehen Spuren im eigenen Rechner, die man löschen sollte. Außerdem sollte der Rechner mit einem Passwort geschützt sein, das weder ein Eigenname noch ein Begriff aus dem Lexikon ist. Schließlich müssen die Anbieter ihre Kunden über Sicherheit aufklären.
SZ: *T-Online behauptet, seine Kunden würden ausreichend informiert.*
Kongehl: Nicht ausreichend, meine ich. Die Provider wollen, daß die Leute möglichst viel surfen und da ist Sicherheit ge-

Pressemeldung 1: Süddeutsche Zeitung 9./10. April 1998

Vor Aushöhlung des Datenschutzes gewarnt

Datenschützer kritisieren: Viele Unternehmen setzen keine Beauftragten ein

Viele Unternehmen und Institutionen kommen nach Ansicht deutscher Datenschützer nicht der gesetzlichen Verpflichtung nach, Datenschutzbeauftragte einzusetzen. Rund 20 Prozent aller großen und mittelgroßen Unternehmen in Deutschland beschäftigen nach Angaben des Vorsitzenden des Bundesverbandes der Datenschutzbeauftragten Deutschlands (BvD), Gerhard Kongehl, kein entsprechendes Personal. Bei kleinen Betrieben seien es deutlich mehr als die Hälfte, sagte Kongehl während einer Fachtagung seines Verbandes in Ulm. Grund dafür seien unter anderem fehlende Kontrollen. Theoretisch sind Firmen ab fünf Personen verpflichtet, einen Datenschutzbeauftragten einzusetzen.

Der Bundesverband forderte auf der Tagung zudem eine eigenständige Berufsausbildung. Mit der rasanten Weiterentwicklung von Informations- und Kommunikationstechnologien komme den Datenschützern in Unternehmen und Institutionen eine immer wichtigere Rolle zu, sagte Kongehl. Die Anforderungen an technische und gesetzliche Kenntnisse der Beauftragten wüchsen ständig. Bislang müssen Datenschutzbeauftragte keine besondere Berufsqualifikationen für ihre Aufgabe mitbringen.

Kongehl sprach sich auch dafür aus, die Arbeit der Datenschützer in den Unternehmen auf eine bessere rechtliche Grundlage zu stellen. Ein Beauftragter, der wie bisher nur Empfehlungen aussprechen könne, sei nicht mehr zeitgemäß. „Wir müssen aufpassen, daß wir nicht zu Fossilien der modernen Informationsgesellschaft werden." Er forderte für die Datenschutzexperten ähnliche Kompetenzen, wie sie Betriebsräten zukommen. Eine Novellierung des Bundesdatenschutzgesetzes (BDSG) sei längst überfällig, sagte Kongehl, der an der Fachhochschule in Ulm lehrt.

Der Datenschutzbeauftragte des Landes Baden-Württemberg, Werner Schneider, warnte nachdrücklich vor einer weiteren Aushöhlung des Datenschutzes. Die schnelle Verbreitung moderner Kommunikationstechniken wie des weltweiten Computernetzes Internet berge ungeahnte Möglichkeiten der Ausforschung und Beeinflussung. Der sogenannte große Lauschangriff treffe vor allem unbescholtene Bürger, kritisierte Professor Ulrich Stephan von der Polizei-Fachhochschule Villingen-Schwenningen. Gegen die organisierte Kriminalität sei mit den bestehenden Abhör- und Kontrollmöglichkeiten kaum noch etwas auszurichten, da diese sich mittlerweile modernster Abwehrtechniken bedienten.

Um die Qualifikation künftiger Generationen von Datenschützern zu verbessern, schlug der BvD-Vorsitzende Kongehl langfristig eine eigenständige Ausbildung zum Datenschutzbeauftragten vor. Vorstellbar sei beispielsweise ein achtsemestriges Studium an einer Fachhochschule zum diplomierten Sicherheitsingenieur. Die Hochschule für Technik in Ulm ist nach seinen Angaben die erste, die seit zehn Jahren eine Ausbildung für Datenschützer in Form einer Weiterbildung für Informatiker anbietet.

Rund 60 Datenschützer aus ganz Deutschland diskutierten in Ulm über die Zukunft ihres Berufsstandes. Dem 1989 gegründeten Bundesverband der Datenschutzbeauftragten Deutschlands gehören rund 200 Mitglieder an. lsw

Pressemeldung 2: Staatsanzeiger für Baden Württemberg 8. April 1998

Datenschützer rügen Firmen

„Oft nur Alibi-Funktion" – Viele Computer nicht gesichert

Ulm (gük). Mehr Kompetenzen für die Datenschützer in den Unternehmen fordert der Bundesverband der Datenschutzbeauftragten. Viele Kollegen seien oft zahnlose „Papiertiger mit Alibi-Funktion", kritisierte der Vorsitzende des Verbandes, Kongehl. Er fordert für Datenschützer verbindliche Richtlinien, wie es sie auch für Betriebsärzte gebe.

Der Lauschangriff und das Internet, aber auch die flächendeckende Verbreitung von Mobiltelefonen, Kredit-, EC- und Geldkarten machen den Bürger nach Ansicht des Ulmer Professors zum gläsernen Menschen. So habe der Erotikversand Beate Uhse jahrelang die Adressen seiner Stammkunden an Adreßhändler weitergegeben, kritisierte Kongehl bei einer Tagung in Ulm. Diese hätten die Telefonbücher dann nach Pfarrern unter den Kunden durchforstet – und Geistliche erpreßt.

Auch das bargeldlose Bezahlen mit Kredit- oder Geldkarte hinterlasse ebenfalls Datenspuren, sagte Kongehl. Wer zum Beispiel regelmäßig in einer Edelboutique einkaufe oder in einer Luxusherberge übernachte, die von der Mafia als Geldwaschanlage benutzt werde, laufe schnell Gefahr, in den Kreis der Verdächtigen aufgenommen zu werden.

Daß Daten-Räuber meist einfaches Spiel haben, hat Kongehls Team bewiesen: Von 6000 im Raum Ulm überprüften Rechnern mit Internet-Zugang, darunter in Arztpraxen, Polizeirevieren, Firmen und Anwaltskanzleien, war nur jeder achte Computer vor dem Zugriff von Hackern ausreichend geschützt.

Pressemeldung 3: Illertisser Zeitung 1. April 1998

Kongehl: Gläserner Bürger ist längst Wirklichkeit

Datenschützer warnt vor vollständigem Verlust an Privatheit

Ulm (gük). Auf dem Weg in eine voll digitalisierte und vernetzte Gesellschaft werden schon in den nächsten Jahren „so ziemlich alle der bisher noch verschonten Lebensbereiche des Menschen belauschbar, überwachbar und registrierbar". Dieses beunruhigende Szenario entwarf der Ulmer Professor Gerhard Kongehl bei der Jahreskonferenz der Datenschutzbeauftragten, die seit gestern in der Donaustadt tagen.

Wie sehr der gläserne Bürger schon Wirklichkeit ist, mußte Kongehl, der Vorsitzender des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) ist, am eigenen Leib erfahren. Aus heiterem Himmel bekam er von seiner Krankenversicherung einen Risikozuschlag aufgebrummt. Seine Nachfrage ergab, daß er inzwischen als Diabetiker geführt wurde. Warum? Weil er einen Blutzukkertest durchführen ließ, der allerdings keine Hinweise auf eine Diabetes-Erkrankung ergeben hatte. Um die falsche Datenspur zu löschen, mußte Kongehl die Untersuchung noch einmal über sich ergehen lassen.

Der Datenschutzexperte könnte noch viele Beispiele nennen, bei denen massiv in die Privatsphäre der Bürger eingegriffen wird, so zum Beispiel die Überwachung des Ulmer Münsterplatzes mit einer Videokamera. Eigentlich, so glaubt er, müßte das Thema daher Hochkonjunktur haben. Doch dem sei beileibe nicht so. Kongehl diagnostiziert eine „Duldungsstarre" der Gesellschaft, die eine „verheerende Verluderung des Datenschutzes" in Kauf nehme.

Die Gründe dafür seien vielschichtig. Zum einen werde es immer schwieriger, den technischen Fortschritt zu bändigen. „Der Verlust an Privatheit vollzieht sich scheibchenweise", sagt Kongehl. „Die neuen Gefahren kündigen sich nicht mit einem Paukenschlag an, sie schleichen sich ein, entfernen sich immer mehr von der wahrnehmbaren Welt." Zum anderen trage die Globalisierung der Wirtschaft, die Massenarbeitslosigkeit und die damit verbundene Diskussion um den Standort Deutschland zum schlampigen Umgang mit sensiblen Daten bei. Es entstehe der Eindruck, daß man sich hierzulande ein informationelles Selbstbestimmungsrecht des Bürgers aus Wettbewerbsgründen nicht mehr leisten könne: „Erst kommt das Fressen, dann die Moral."

Ein drittes Manko sei der geringe Stellenwert, den der Datenschutz in Unternehmen und Behörden genieße. Häufig werde auf mehr oder weniger kreative Weise versucht, sich diesen vom Hals zu schaffen. Externe „Tele-Datenschützer", von gewieften Unternehmensberatern als Geheimtip gehandelt, seien eine „Farce", weil sie niemals in der Lage seien, gleich in einer ganzen Reihe von Firmen für Datensicherheit zu sorgen.

Aussichtslos sei der Kampf gegen Datenmißbrauch dennoch nicht, zumal Deutschland im internationalen Vergleich nicht schlecht abschneide. Um den Kampf zu gewinnen, müßten allerdings datenschutzfreundliche Techniken verstärkt zum Einsatz kommen und deren Entwicklung finanziell gefördert werden. Kongehl fordert ferner mehr Personal für die Datenschutzbeauftragten der Bundesländer, vor allem aber eine Debatte über die Frage, welche Daten aus Gründen der inneren Sicherheit wirklich gespeichert werden müssen.

Pressemeldung 4: Neu Ulmer Zeitung 31. März 1998

Tag der offenen Daten-Tür bei der Ulmer Polizei?

Verband der Datenschützer nahm 6000 Computer unter die Lupe – Nur jeder achte Rechner ist vor Hackern sicher

Von unserem Mitarbeiter Günter Kast

Ulm

Wie sicher sind die Daten in Arztpraxen, Drogenberatungsstellen, Anwaltskanzleien, Unternehmen und bei der Polizei? „Erschütternd unsicher" sagen die Datenschützer, deren Berufsverband derzeit im Stadthaus Ulm seinen Jahreskongreß abhält (siehe separater Bericht). Bei einem Praxistest fanden sie heraus: Jeder Tag im Internet ist ein Tag der offenen Tür, nur jeder achte der 6000 überprüften Rechner ist vor Datenräubern gefeit. Die Polizeidirektion Ulm weist diesen Vorwurf zurück. Deren Sprecher: „Unsere Daten sind sicher."

Daß es Anfang der Woche zwei 16jährigen Hackern gelungen ist, in den Datenbanken der T-Online-Benutzer zu stöbern, wundert den an der Fachhochschule Ulm lehrenden Professor Gerhard Kongehl nicht. Der Vorsitzende des Bundesverbandes der Datenschutzbeauftragten und sein Team haben in einem Großversuch 6000 Computer „gescannt", die über ein Modem erreichbar und damit internet-fähig sind. Das erschreckende Ergebnis: Nur jeder achte Rechner verfügte über Sicherheits- Mechanismen, die für Hakker ein ernstzunehmendes Hindernis darstellen. Die meisten der sogenannten „firewalls", zu deutsch Brandschutzmauern, erwiesen sich als wirkungslos.

Bei den Datenschützern gab es daraufhin eine lebhafte Diskussion darüber, ob man den Versuch weiterführen und tatsächlich Einblick in Patientendateien, Unternehmens-Bilanzen und vertrauliche Mitteilungen im Polizei-Computer nehmen soll. Kongehl: „Letztendlich haben wir gesagt: 'Wir dürfen da nicht weiter.'" Daß es tatsächlich möglich ist, in die mit einem Modem verbundenen Rechner einzudringen, bewies der Süddeutsche Rundfunk. Bei einem Ulmer Unternehmen konnten die Journalisten ungestört Auftrags-Angebote und Rechnungen studieren.

Wolfgang Jürgens, der Sprecher der Ulmer Polizeidirektion (PD), weist die Vorwürfe der Datenschützer indes vehement zurück. Der Landesbeauftragte für den Datenschutz in Baden-Württemberg, Werner Schneider, habe ihm bei einer Visite ausdrücklich bestätigt, daß die gespeicherten Daten sicher seien. Jürgens räumt zwar ein, daß es möglich sei, in einen Rechner einzudringen, wenn dieser via Modem mit dem Internet verbunden ist. Die PD treffe dagegen jedoch Vorsorge, indem sie eine physikalische Trennung von Internet-Zugang und allen internen Datenträgern (Intranet) herbeiführe. Jürgens: „Sobald wir im Web sind, wird die Leitung zu den internen Daten gekappt."

Unter Experten ist jedoch umstritten, ob „firewall"-Sicherungen einen ausreichenden Schutz vor Datenräubern bieten. Diese können nämlich sogenannte trojanische Pferde einschleusen und damit in den Besitz eines Schlüssels zu einer fremden „Wohnung" kommen, mit dem sich auch nachträglich und trotz der Trennung von Intra- und Internet Türen öffnen lassen, die den Zugang zu sensiblen Daten ermöglichen. Um das trojanische Pferd zu aktivieren, muß es allerdings, so PD-Sprecher Jürgens, „jemand geben, der dem Pferd in den Po stupft," – der nicht nur eine Lese- und Zugriffs-, sondern auch eine Schreibberechtigung für den betreffenden Rechner hat. Und über diese Berechtigung verfügten eben nur die Beamten der Polizeidirektion, nicht aber daten-hungrige Computer-Piraten.

Die Ulmer Datenschützer können diese Argumente nicht vollends überzeugen. Sie bieten deshalb der PD Ulm ihre Dienste und ihr technisches Know-How an, um die bei den Ordnungshütern gespeicherten Personendaten vor Schnüfflern zu schützen. Kongehl: „Wir hätten da Lösungsmöglichkeiten." Er sei allerdings skeptisch, ob die PD das Angebot annehmen werde.

Wie aktuell das Thema Daten(un)sicherheit ist, zeigt ein anderes Beispiel: Vor kurzem erging an alle Betreiber von Bürgernetzen in „Bayern Online" und damit auch an das Bürgernetz Ulm/Neu-Ulm der „technische Hinweis", daß der gesamte Inhalt der e-mail-Server regelmäßig zu sichern, zwölf Monate aufzubewahren und für gezielte Recherchen der Strafverfolgungsbehörden bereitzustellen sei. Bei ISDN-Anschlüssen soll zusätzlich der Anschluß protokolliert werden, von dem aus die „Sitzungen" durchgeführt wurden.

Pressemeldung 5: Neu Ulmer Zeitung 1. April 1998

DATENSCHUTZKONGRESS

Ein Relikt der Computerzeit

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) veranstaltet heute und morgen von 9 Uhr an im Ulmer Stadthaus einen Datenschutzkongreß. Alle Datenschützer und Datenschutzinteressierten sind eingeladen sich an den zwei Kongreßtagen über den neuen Lauschangriff und die Rolle der Datenschutzbeauftragten im Multimedia-Zeitalter zu informieren.

Wird der Datenschutzbeauftragte ein Relikt der Computersteinzeit werden? Als erste Hochschule in Deutschland hat die Fachhochschule Ulm vor zehn Jahren angefangen, Datenschutzbeauftragte auszubilden. Dieses „Ulmer Modell" war wegweisend für andere Hochschulen. Der BvD feiert nun das zehnjährige Bestehen des Ulmer Modells am Ort seines Entstehens.

Pressemeldung 6:

Südwest Presse 31. März 1998

Firmen scheuen den Datenschutz

ULM (lsw) - Viele Unternehmen und Institutionen kommen nach Darstellung deutscher Datenschützer nicht der gesetzlichen Verpflichtung nach, Datenschutzbeauftragte einzusetzen. Rund 20 Prozent aller großen und mittelgroßen Unternehmen in Deutschland beschäftigen nach Angaben des Vorsitzenden des Bundesverbandes der Datenschutzbeauftragten Deutschlands (BvD), Gerhard Kongehl, kein entsprechendes Personal. Bei kleinen Betrieben seien es deutlich mehr als die Hälfte, sagte Kongehl auf einer Fachtagung seines Verbandes am Dienstag in Ulm. Grund dafür seien unter anderem fehlende Kontrollen. Firmen von fünf Personen an seien aber verpflichtet, einen Datenschutzbeauftragten einzusetzen. Der Bundesverband forderte eine eigenständige Berufsausbildung. Mit der rasanten Weiterentwicklung von Informations- und Kommunikationstechnologien komme den Datenschützern in Unternehmen und Institutionen eine immer wichtigere Rolle zu, sagte Kongehl. Die Anforderungen an technische und gesetzliche Kenntnisse der Beauftragten wüchsen ständig. Bislang müssen Datenschutzbeauftragte keine besondere Berufsqualifikationen haben.

Pressemeldung 7:

Schwäbische Zeitung 1. April 1998

DATENSCHUTZ / Testlauf bringt erstaunliche Erkenntnisse

Durch offene Türen ins Polizei-Netz

Datenbanken von Behörden und Ämtern schlecht gesichert?

Sind die Daten der Ulmer Polizei sicher? Einem Computerspezialisten ist es in Zusammenarbeit mit einem Fernsehteam gelungen, sich über das Internet bei der Ulmer Polizei einzuklinken. Doch die winkt ab: Ein Zugriff auf die gespeicherten Daten sei nicht möglich.

HANS-ULI MAYER

Der Berufsverband der Datenschutzbeauftragten (BvD), dem der Ulmer Professor Gerhard Kongehl vorsteht, äußert schon lange den Verdacht, daß Computer-Daten nicht ausreichend gesichert seien. Ende Januar haben ein Ulmer Ingenieur und ein Team des SDR-Fernsehens die Probe aufs Exempel gemacht und darüber einen Film gedreht, der am Montag rechtzeitig zum Beginn einer Fachtagung im Stadthaus ausgestrahlt wurde. In Absprache mit der Stadt Ulm durchforschten sie das lokale Netz und fanden Erstaunliches.

Zufällig waren sie bei ihren Recherchen auf einen Rechner mit dem Namen „PD Ulm" (PD=Polizeidirektion) gestoßen und hatten sich eingewählt: „Wir sind nur durch offene Türen gegangen", beschreibt der Computerspezialist sein Vorgehen. Und: „Es gab keinerlei technische Hindernisse." So seien die drei Festplatten, die er vorgefunden habe, nicht einmal mit den üblichen Paßworten gesichert gewesen.

Bemängelt die Sicherung von Computer-Daten: Professor Gerhard Kongehl auf dem BvD-Kongreß in Ulm.

Informationen sind aber nicht eingesehen worden. In dem Testlauf sei aber dokumentiert worden, daß 10 bis 15 Prozent der überprüften Computer von Privatpersonen, Behörden und Ämtern falsch oder unzulänglich gesichert seien.

Die Ulmer Polizei ist in diesem Bemängelt die Sicherung von Computer-Daten: Professor Gerhard Kongehl auf dem BvD-Kongreß in Ulm.Zusammenhang nur zufällig ausgewählt worden und nur ein Beispiel, wie der Fernseh-Journalist Uli Andelfinger sagt. Die Netz-Türen standen genauso bei anderen Behörden und bei Unternehmen offen. In einem Fall seien in einem Firmencomputer sogar „vertrauliche Mitteilungen" zu lesen gewesen.

Für Ulms Polizeisprecher Wolfgang Jürgens ist die Aufregung nicht nachvollziehbar: „Bei uns ist kein externer Zugriff auf Daten möglich." Zwar bestätigt er, daß sich die Polizei bei ihrer Ermittlungsarbeit auch des Internets bediene. Bis auf einen Computer hätten diese Geräte aber keinen Anschluß an das interne Datennetz. Lediglich in einem Fall sei dies gegeben, da aber seien keine sensitiven Daten gespeichert. Im übrigen seien „physikalische Sperren" eingebaut, die auch mit technischen Finessen, wie etwa dem sogenannten „Trojanischen Pferd", nicht zu überwinden seien. „Wir sind auf einem hohen Sicherheitsstandard", sagt er und fügt an, daß selbst der Landesbeauftragte für Datenschutz das Ulmer System unlängst für sicher befunden habe.

Holger Heimann vom Vorstand des Berufsverbandes hat da aber so seine Zweifel. Der Ulmer Ingenieur und Daten-Sicherheitsberater bemängelt, daß bei der Polizei keine Netzwerk-Fachleute arbeiten würden. Es sei ein Fehler gewesen, keine Paßwörter zu vergeben und so seien auch andere Fehler möglich. Heimann: „So etwas muß ein Profi begleiten."

Pressemeldung 8: Südwest Presse 1. April 1998

····· Letzte Seite ·····

Personalien

Der Justitiar des BvD, Dr. Armin Herb, wurde kürzlich von der Fachhochschule Ulm zum Honorarprofessor ernannt. Der Vorstand des BvD beglückwünscht Herrn Dr. Herb und wünscht ihm auch weiterhin viel Erfolg.

Vorschau: Mitgliederzeitung 3/98

In der nächsten Ausgabe gibt es den zweiten Teil der Kongreßreferate.

Unser Ju§titiar, Herr Herb wird bis dahin einen Kommentar zur angeblichen „hypertrophy“ des Datenschutzes verfassen.

Außerdem wird es Vorschläge des BvD zur Novellierung des BDSG geben.

Impressum

Mitgliederzeitung des Berufsverbandes der Datenschutzbeauftragten e.V. (BvD)

Herausgeber: Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)

Ausschuß für Öffentlichkeitsarbeit:
Dr. Manfred Baumeister, Markus Mix

Redaktionelle Bearbeitung: Markus Mix

Geschäftsstelle:
Berufsverband der Datenschutzbeauftragten e. V.
Ehingerstr. 19
89077 Ulm

Tel: 0731/6026265
Fax: 0731/9608511
WWW: http://www.fh-ulm.de/bvd/bvd.html
E-Mail: bvd@fh-ulm.de

Verteiler: bvd-forum@ibh.tfu.uni-ulm.de
(Offene E-Mail-Verteilerliste zu Fragen des Datenschutzes)

V.i.s.d.P. Prof. Dr. Gerhard Kongehl