Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 87 (1996)

Heft: 3

Artikel: Anmerkungen aus der Sicht des Eidg. Datenschutzbeauftragten (EDSB) zum Bulletin-Beitrag "Im PC-Dschungel"

Autor: Scherrer, Urs

DOI: https://doi.org/10.5169/seals-902301

Anmerkungen aus der Sicht des Eidg. Datenschutzbeauftragten (EDSB) zum Bulletin-Beitrag «Im PC-Dschungel»

Im PC-Dschungel

Der im Bulletin SEV/VSE 21/95 publizierte Beitrag von *bau* befasst sich mit den Problemen, auf welche der Schreibende bei einem Importeur von PC-Material stiess, als er seine defekte Harddisk während der Garantiezeit zur Reparatur übergeben musste. Was geschieht mit der defekten Harddisk? Wie stellt man sicher, dass die Daten nicht in unbefugte Hände fallen? Das waren die Fragen, die er über den Händler dem Importeur stellen liess. Erstens gebe es für den Erhalt der Daten keine Garantie, zweitens wisse man nicht, wie man eine Löschung bewerkstelligen solle, und drittens müsse man die defekte Disk dem Hersteller zurückschicken, damit dieser Garantieersatz leiste. Das Schönste an der Geschichte war, dass nach Insistieren des Kunden die Harddisk gelöscht werden konnte – weil nur die leicht auswechselbare Elektronik, nicht aber die Harddisk defekt war. Die uns vom Importeur versprochene Stellungnahme ist bis heute leider ausgeblieben.

Freundlicherweise aber haben wir vom Eidg. Datenschutzbeauftragten eine Stellungnahme erhalten, die wir nachstehend mit bestem Dank an die hilfreiche Bundesstelle wiedergeben.

SEV, Bulletin-Redaktion

Ausgangslage

Der im Titel aufgeführte Artikel (siehe Kasten) tangiert in folgenden Bereichen das Datenschutzgesetz (DSG[1]):

- Datensicherheit (insbesondere Vertraulichkeit)
- Löschen der Daten
- Datenbearbeitung durch Dritte
- Bekanntgabe[2] der Daten ins Ausland

Das DSG gilt für private Personen und für Bundesorgane und ist anwendbar bei jeglicher Datenbearbeitung, bei der Personendaten[3] bearbeitet werden. In den allgemeinen Datenschutzbestimmungen (Abschnitt 2 des DSG) ist in Art. 7 Abs. 1 festgehalten:

«Personendaten müssen durch angemessene[4] technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten[5] geschützt werden.»

Vertraulichkeit der Daten (Chiffrierung)

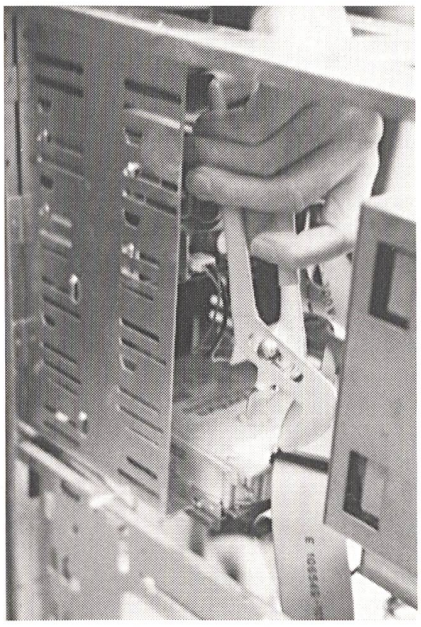
Das vorliegende Beispiel (Kasten) zeigt die Vorteile einer Chiffrierung auf. Der Inhaber der Datensammlung[6] hat unter anderem auch bei Reparaturen die Gewissheit, dass die von ihm erstellten Daten nicht eingesehen bzw. interpretiert werden können. Eine Chiffrierung der Daten kann aber nie als vollständig sicher betrachtet werden, weil auch diese Daten mit entsprechend hohem Aufwand[7] entschlüsselt werden können.

Löschen der Daten

Will man die Informationen auf magnetischen Datenträgern vollständig löschen, so muss nicht nur eine logische, sondern eine physische Löschung der Daten erfolgen. Die DOS-Befehle ERASE und DELETE löschen nur logisch. Die Daten können mit dem Befehl UNDELETE wieder erstellt werden, wenn in der Zwischenzeit nicht der logisch gelöschte Bereich der Diskette überschrieben wurde. Die Löschung einer Diskette mit dem Befehl FORMAT kann ohne die Angabe des Parameters /U mit dem Befehl UNFORMAT rückgängig gemacht werden. Kann aber die Disk wegen des Defekts nicht mehr «herkömmlich» angesprochen werden, so müssen andere Massnahmen ergriffen werden, damit die Daten auf der Disk gelöscht werden können. Eine Möglichkeit besteht darin, mit sehr grossen magnetischen Wechselfeldern die Informationen auf den Datenträgern zu löschen. Erst dann sind die Daten physikalisch gelöscht und können nicht mehr rekonstruiert werden.

Sicherheitskopien (Backup)

Ein Defekt der Festplatte kann dazu führen, dass die Daten auf dieser nicht mehr hergestellt werden können. Aus diesem Grunde empfiehlt es sich, in regelmässigen Abständen insbesondere von den selbsterstellten Daten Sicherheitskopien (Backup) anzulegen.



Besteht die einzig sichere Löschung in der physischen Elimination des Datenträgers?

[1] SR 235.1

[2] Bekanntgeben: das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen.

[3] Personendaten (Daten): sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

[4] Der Begriff angemessen führte insbesondere im technischen Umfeld zu Diskussionen. In dem vom Eidg. Datenschutzbeauftragten herausgegebenen Leitfaden zu den technischen und organisatorischen Massnahmen wird festgehalten, wie eine angemessene Einstufung in Datensicherheitsstufen vorgenommen werden kann.

[5] Bearbeiten: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

[6] Inhaber der Datensammlung: private Person oder Bundesorgane, die über den Zweck und den Inhalt einer Datensammlung entscheiden.

[7] Prof. Dr. Ueli Maurer von der ETH Zürich nimmt in der von ihm verfassten Studie «Sicherheit in Datennetzen» in der Sondernummer 1/1996 der Publikation Fakten (Zeitschrift für Datenschutz des Kantons Zürich) zu Chiffrierverfahren wie folgt Stellung: «Der Schlüssel von DES beträgt 56 Bit, d. h. es gibt $2^{56} \approx 7{,}2 \cdot 10^{16}$ verschiedene Schlüssel. Diese Schlüsselgrösse ist gerade an der Grenze dessen, was sich mit massiven Computerressourcen in realistischer Zeit durchprobieren lässt. DES ist also gegen normale Hacker (noch) sicher, die Geheimdienste können DES aber bestimmt innert weniger Minuten oder Stunden brechen. Tatsächlich wurde möglicherweise die Schlüsselgrösse von der amerikanischen National Security Agency (NSA) aus diesem Grund so klein gewählt, denn der ursprüngliche Vorschlag von IBM enthielt einen 64-Bit-Schlüssel, was immerhin 256mal sicherer wäre.
Ab etwa 80 Schlüsselbits kann ein Chiffriersystem auch gegen mächtige Geheimdienste sicher sein, sofern er keine strukturellen Schwächen aufweist. Viele der im kommerziellen Bereich verkauften Algorithmen sind nicht wirklich sicher, einige sogar sehr schwach. Die amerikanische Regierung gestattet nur den Export von Systemen mit höchstens 40-Bit-Schlüssel (für den Export von DES mit 56-Bit-Schlüssel muss eine spezielle Genehmigung eingeholt werden). Solche Systeme müssen als ziemlich unsicher angesehen werden.
Zwei Algorithmen, die höchste Sicherheit aufweisen, sind IDEA und Triple-DES (dreifache Anwendung von DES). Allerdings lässt sich bis heute die Sicherheit keines dieser Systeme mathematisch beweisen.

Datenbearbeitung durch Dritte

Wird eine Harddisk zur Reparatur an Dritte (Händler oder Servicestelle) weitergegeben, so gelten auch für diese die Datenschutzbestimmungen, wie zum Beispiel Art. 7 (siehe Ausgangslage). Eine vertragliche Wegbedingung von allgemeinen Datenschutzbestimmungen gegenüber dem Kunden, zum Beispiel mit dem Argument des Vertrauens (bei uns passiert nie etwas) kann für den Händler (Servicestelle) Folgen haben, wenn dadurch die Persönlichkeit der Betroffenen beeinträchtigt wird. Andererseits trägt auch der Inhaber der Datensammlung Verantwortung, wenn er Daten durch Dritte bearbeiten lässt. In Art. 14 Abs. 1 des DSG wird festgehalten:

«Das Bearbeiten von Personendaten kann einem Dritten übertragen werden, wenn:

a. der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte, und
b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.»

Bekanntgabe von Daten ins Ausland

Die Weitergabe der defekten Harddisk an den Hersteller ist sehr wahrscheinlich mit einer Bekanntgabe der Daten ins Ausland verbunden. In Art. 6 Abs. 2 des DSG ist festgehalten:

«Wer Datensammlungen[8] ins Ausland übermitteln will, muss dies dem Eidg. Datenschutzbeauftragten vorher melden, wenn:

a. für die Bekanntgabe keine gesetzliche Pflicht besteht und (oder)
b. die betroffenen Personen davon keine Kenntnis haben.»

Eine gesetzliche Pflicht wird für die Weitergabe der Harddisks an den Hersteller nicht bestehen. Die betroffenen Personen[9] können voraussichtlich in den meisten Fällen nicht davon in Kenntnis gesetzt werden, dass bei einer Harddisk-Reparatur Personendaten, die sie betreffen, ins Ausland übermittelt werden.

In der Verordnung zum Bundesgesetz über den Datenschutz (VDSG[10]) werden noch Ausnahmen von der Meldepflicht aufgeführt. Art. 7 Abs. 2 lautet wie folgt:

«Die Übermittlung von Datensammlungen in Staaten, die über eine gleichwertige Datenschutzgesetzgebung verfügen, ist nicht meldepflichtig, es sei denn, die Datensammlungen beinhalten besonders schützenswerte Personendaten[11] oder Persönlichkeitsprofile[12], oder eine Weiterleitung in ein Drittland ohne gleichwertige Gesetzgebung sei vorgesehen.»

Eine detaillierte Aufführung der Staaten, die über ein Datenschutzgesetz verfügen, welches mit dem DSG vergleichbar ist, kann beim EDSB bezogen werden.

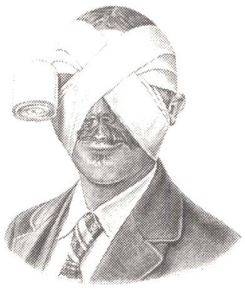
Aufgrund der obigen Angaben sollte man feststellen können, wann eine Datenbekanntgabe ins Ausland beim EDSB angemeldet werden muss.

Urs Scherrer, Mitarbeiter des Eidgenössischen Datenschutzbeauftragten

[8] Datensammlung: jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.
[9] Betroffene Personen: natürliche oder juristische Personen, über die Daten bearbeitet werden.
[10] SR 235.11
[11] Besonders schützenswerte Personendaten: Daten über:
1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
3. Massnahmen der sozialen Hilfe,
4. administrative oder strafrechtliche Verfolgungen und Sanktionen.
[12] Persönlichkeitsprofil: eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Internet-Benutzer dürfen nicht alles sehen

Der Zugang zum Internet mittels SLIP- oder PPP-Verbindungen über ein Modem oder ISDN durch einen kostenpflichtigen Service-Provider garantiert zur Zeit nicht den vollen Zugriff auf alle Informationen. Im Verlauf des vergangenen Jahres sind die Anbieter von Internet-Zugängen dazu übergegangen, ihren Kunden gewisse Informationsbereiche vorzuenthalten. Sie tun dies präventiv aus Furcht vor juristischen und polizeilichen Interventionen, weil sie befürchten, für illegale oder unsittliche Internet-Inhalte ins Recht gefasst zu werden.



Die Tatsache und das Ausmass der Sperren sowie Details zur Art der nicht vermittelten Inhalte werden den zahlenden Kunden in der Regel verheimlicht. Das ist nicht verwunderlich, zumal der ursprüngliche Servicevertrag normalerweise einen vollständigen Zugang zum Internet vorsieht und kaum ein Provider die Reduktion seines Dienstes zum Anlass für eine Gebührensenkung genommen hat. Die Sperrungen sind teilweise sehr umfangreich und rigoros. Auf Anfrage bestätigen sie manche der Schweizer Zugangsdienste, andere geben sie nur indirekt zu, indem sie auf «gesetzliche Vorschriften» verweisen.

Fälschung als Auslöser

Anlass für die Sperren ist die von den Medien verbreitete und von Politikern und Justizbehörden für bare Münze genommene Behauptung, das Internet transportiere hauptsächlich pornographische Inhalte und diene einer weltweit operierenden Bande von Pädophilen und Kinderschändern zur Ausübung unsäglicher Verbrechen. In der Schweiz war es das Nachrichtenmagazin «Facts», welches diese Story verbreitete. Sie beruhte auf einer nachweislichen und bewussten Fälschung eines amerikanischen Studenten namens Marty Rimm, auf die vorher bereits das US-Magazin «Time» hereingefallen war. In einem Coup, ähnlich der Affäre um die Hitler-Tagebücher in Deutschland, hatte der an der Carnegie-Mellon-Universität von Pittsburgh eingeschriebene Rimm der Zeitschrift ein von A bis Z erfundenes Machwerk über «Cyberporn» für eine Titelstory untergejubelt.

«Time» entschuldigte sich wenig später bei seinen Lesern und dementierte die absurde Geschichte vollumfänglich. In der Schweiz hingegen wurde sie der Öffentlichkeit als «Untersuchung der Carnegie-Mellon-Universität» präsentiert. «Facts» warf Polizei und Justiz vor, technisch rückständig zu sein und angesichts eines üblen elektronischen Pornohandels untätig zu bleiben. Das Magazin forderte, dass endlich gegen das Internet vorgegangen werde. Umgehend wurde der Zürcher Staatsanwalt Ulrich Weder aktiv. Es wurde eine Anzahl Computer einer Zürcher Hobby-Mailbox beschlagnahmt, die allerdings nicht ans Internet angeschlossen waren. Über den weiteren Verlauf dieses Verfahrens wurde nichts mehr bekannt.

Ermittlungen gegen Compuserve

Ähnliches spielte sich Ende Jahr in Bayern ab. Dort kreuzte am 22. November die Polizei mit einem Durchsuchungs- und Beschlagnahmebeschluss in den Räumen des weltweiten Datendienstes Compuserve in Unterhaching bei München auf und eröffnete der verdutzten Bedienungsmannschaft, gegen sie werde wegen Verbreitung von Kinderpornographie ermittelt. Zuvor