die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

ISSN 0930-1054 • 2010
2500000000 µcent

#100

Mitglied nicht verlangen, dass sein Mitgliedsdatensatz gelöscht wird. Aber es können Informationen, die rechtlich nicht notwendig sind, aus dem Datensatz gelöscht werden. Immer dann, wenn die Daten nicht gelöscht werden können, besteht ein Recht auf einen Sperrvermerk.

Auftragsverarbeitung

Wenn der Club einem Dienstleister Aufgaben überträgt und dabei auch die Weitergabe von Mitgliederdaten notwendig ist, dann ist ein Vertrag über diese Auftragsverarbeitung abzuschließen.

Beispielsweise ist ein Vertrag abzuschließen, wenn durch einen Dienstleister der Versand von Mitgliederschreiben oder Datenschleudern durchgeführt wird. Auch wenn die Mitgliederdaten bei einem Dienstleister gehostet werden, ist zu prüfen, ob ein Auftragsverarbeitungsvertrag abzuschließen ist.

Der Club muss dabei darauf achten, dass zur Absicherung der Mitgliederdaten ein ausreichender Schutz vorhanden ist. Es müssen dem Schutzbedarf der personenbezogenen Daten angemessene technische und organisatorische Maßnahmen ergriffen werden.

Technische und organisatorische Maßnahmen

Doch nicht nur bei der Auftragsverarbeitung, sondern auch bei der Verarbeitung von personenbezogenen Daten im Club-Umfeld sind diese technischen und organisatorischen Maßnahmen anzuwenden. Zu den technischen Maßnahmen gehören beispielsweise Maßnahmen wie Alarmanlage, Verschlüsselung sowie die Protokollierung von Erfassung und Änderung personenbezogener Daten. Zu den organisatorischen Maßnahmen gehören beispielsweise das Führen eines Gästebuchs, das Vier-Augenprinzip und ein Berechtigungskonzept.

Die Art der jeweiligen Maßnahme ist vom Schutzbedarf der zu schützenden Daten abhängig. D. h. es sind die Auswirkungen bei Nichtgreifen einer Maßnahme auf den Betroffenen zu bewerten. So sind bei Bekanntwerden einer Erkrankung die möglichen Auswirkungen für einen Betroffenen in der Regel höher als wenn der Name unbeabsichtigt veröffentlicht werden würde.

Fazit

Der Club, die lokalen Erfa-Kreise und die Chaostreffs sollten ihre Augen nicht vor den regulatorischen Vorgaben rund um den Datenschutz verschließen. Die Regelungen des Datenschutzes gelten auch für nicht eingetragene Vereine und ein Nichteinhalten kann zu Auflagen oder Bußgeldern gegenüber dem Club, aber auch gegenüber den Verantwortlichen führen. Zum Start sind einige „Papiertiger"-Tätigkeiten durchzuführen, die dann kontinuierlich weitergeführt werden sollten.

Wer hierzu Rückfragen hat oder Hilfestellung benötigt darf sich gerne an mich wenden, ich unterstütze gerne die lokale Umsetzung.

Referenzen

[1] „Praxisratgeber für Vereine" (2018), https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf

[2] „Forderung Datenbrief des CCC", https://www.ccc.de/datenbrief

[3] Bildquelle: https://de.m.wikipedia.org/wiki/Datei:Herne_Stadtarchiv_alte_Akten.jpg

[4] Bildquelle: https://www.flickr.com/photos/mennonitechurchusa-archives/6987770030/

CCC tuwat Arbeitsgruppe „Kritische Infrastrukturen"

von HonkHase <manuel@atug.de> und ijon <ijon@c-base.org>

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. *Hinweis:* eine Übersicht über die verwendeten Akronyme findet sich auf Seite 0x1D.

Im Sinne des BSI-Gesetz [1] werden Kritische Infrastrukturen wie folgt definiert:

> *Kritische Infrastrukturen [...] sind Einrichtungen, Anlagen oder Teile davon, die*
> 1. *den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und*
> 2. *von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*
>
> *[...]* BSIG § 2, Abs. 10

Dazu kommen noch die Sektoren „Staat und Verwaltung" sowie „Medien und Kultur". Genaueres dazu definiert über das BSIG hinaus die „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" [BSI-KritisV; 2].

Wir als Bürger sind gegenüber Kritischer Infrastruktur machtlos. Wir haben keinen direkten und unmittelbaren Einfluss auf den Betrieb im Regelfall oder im Krisenfall. Das Vertrauen in dieses hohe Gut der Verantwortung haben wir an den Staat abgegeben.

Kritische Infrastruktur wird natürlich ebenfalls durch IT umgesetzt, die nie 100 %ig sicher betrieben werden kann. Wir haben es hier leider nicht mit einer konkreten Einzelfall-Betrachtung zu tun wie bei PC-Wahl[3] oder O'Zapftis [Staatstrojaner; 4], sondern mit Anlagen, die beispielsweise sehr komplex, Jahrzehnte alt, von einem Monopolisten betrieben, Unikate, SCADA oder auch IoT sind. Oftmals unterliegen die Systeme sogar mehreren der genannten problematischen Umstände.

Angegriffene kritische Infrastruktur [12]

Derzeit laufen die Systeme bei uns in Deutschland so zuverlässig, dass (fast) niemand mehr intensive Vorsorge betreibt. Oder fällt Dir spontan ein, wo der nächste öffentliche Trinkwasserbrunnen ist und hast Du

Trinkwasser-geeignete Kanister im Keller? Oder die empfohlene Menge Notfallrationen an Lebensmitteln zu Hause gelagert?

Die Mehrheit der Menschen in Deutschland kann Dir diese Fragen spontan eher nicht beantworten, weil es Wissen ist, dass aufgrund der extremen Seltenheit solcher Ausfälle nicht gebraucht wird [Stichwort „Verletzlichkeitsparadoxon"; 6]. Solche Ausfälle gehören hier in Deutschland nicht zur Lebensrealität, daher hat die Bevölkerung kaum für solche Situationen vorgesorgt.

Wenn also diese Unmenge an Sicherheitslücken in unterschiedlichsten kritischen Systemen wirklich ausgenutzt werden würde und infolgedessen Teile unserer Kritischen Infrastrukturen umfangreich ausfallen, wäre die Bevölkerung hier in Deutschland darauf noch schlechter vorbereitet als in anderen Teilen der Welt. Dort sind Ausfälle grundlegender Infrastruktur ein wiederkehrendes und somit bekanntes Ereignis.

Nehmen wir mal an, dass dieser Fall eintritt. Also jemand (Drittstaaten, Geheimdienste, Terroristen, Blackhats, Script Kiddies ...) nutzt vorhandene Sicherheitslücken aus und schaltet eine signifikante Menge Kritischer Infrastrukturen destruktiv ab...

Wer kommt dann eigentlich der Bevölkerung zu Hilfe?

Es hat den Anschein, als ob die Ressourcen die in dieser Republik vorhanden sind, bei einer Cyberapokalypse nur ein Tropfen auf den heißen Stein wären und vornehmlich nur einen „Staats und Regierungsbetrieb sicherstellen" sollen oder können. Kapazitäten und Ressourcen, die sich um das (nachrangigere?) Ziel von Krisenbewältigung/Krisenschutz (engl. „Disaster Relief" fühlt sich treffender an) gegenüber der Bevölkerung kümmern, sind kaum existent.

Wir haben es also nicht nur mit fehlendem Problembewusstsein zu tun, sondern auch mit einem konkreten Mangel an Ressourcen auf allen Seiten. Ressourcen umfasst hier:

Menschen Zu wenige Menschen wollen was mit Computern für den Staat tun.

Geld Betreiber kritischer Infrastruktur müssen investieren, der Staat muss auch Geld für defensive Schutzmaßnahmen ausgeben, tut er aber bisher nur in zu geringem Maße.

Strukturen Welche Struktur/Organisation käme dann eigentlich und hilft der Bevölkerung?

Prozesse Was tut so eine Struktur/Organisation dann eigentlich als erstes, als zweites, usw. wenn „die Scheiße den Ventilator getroffen" hat?

Da es hier noch Handlungsspielraum und Potential nach oben gibt haben wir uns als tuwat Gruppe Kritische Infrastrukturen zusammengetan, uns ausgetauscht, diskutiert und recherchiert. Und anschließend einen Forderungskatalog zur Verbesserung der Gesamtsituation erarbeitet, den wir euch nicht vorenthalten wollen.

Liste unserer politischen Forderungen

Unabhängigkeit des BSI!

Wir fordern die Unabhängigkeit des BSI vom BMI. Man könnte das BSI wie den Bundesbeauftragten für den Datenschutz direkt dem Bundestag unterstellen. Oder die Rechtsaufsicht verbleibt beim BMI, die Fachaufsicht aber dem BSI, denn die Fach- und Rechtsaufsicht lassen sich teilen – demokratisch. Diese Struktur ist Voraussetzung, dass 3–5-Letter Behörden wie z. B. BfV, BKA, BND, ZITIS und CODE der UniBw oder die von BMVg und BMI gemeinsam neu gegründete „Cyber-militärische Agentur der Bundesregierung" (neudeutsch auch „Agentur für Innovation in der Cybersicherheit" ADIC genannt), nicht von den Mängelberichten, die Betreiber an das BSI melden müssen, profitieren können. Dies ist derzeit z. B. bei Terrorgefahr oder Verdacht auf die Spionagetätigkeit einer fremden Macht der Fall. So würde das Vertrauen der Bürger in das BSI gestärkt und das Amt auch seinem Namen noch besser gerecht werden, denn dann könnte das BSI mit anderen unabhängigen Aufsichtsbehörden wie z. B. der BaFin oder der BNetzA auf Augenhöhe agieren und mehr im Benehmen statt im Einvernehmen agieren. Selbstverständlich dürfen die Know-How-Träger im BSI trotzdem nicht zu anderen Behörden wie z. B. ZITIS, CODE und UniBw abgeworben werden.

Personalausstattung relevanter Behörden!

Wir fordern mehr personelle Ressourcen und fachliche Kompetenzen für BSI, BBK und THW zum Schutz von IT-Komponenten in kritischen Infrastrukturen. Dies erfordert:

- Angemessene Budgets
- Kontinuierliche Ausbildungen und Weiterbildungen
- Nachwuchsförderung

Kompetente Mitarbeiter bekommen die oben genannten nur neu angeworben und gehalten, wenn eine Anpassung des Dienstrechts und der Vergütungsstrukturen vorgenommen wird, um Fachkräfte auch im Wettbewerb mit der Wirtschaft gewinnen zu können. Das bestehende Dienstrecht ist sehr formal und erlaubt die Verbeamtung selbst fähigster IT-Fachkräfte nur in niederen Laufbahngruppen, sofern die notwendigen formalen Laufbahnvoraussetzungen nicht erfüllt sind. Dadurch kann vielen IT-Fachkräften nur eine verhältnismäßig niedrige Besoldung angeboten werden, die am Arbeitsmarkt nicht konkurrenzfähig ist. Eine Flexibilisierung des Laufbahnrechts könnte dieses Problem entschärfen. Im Bereich der Tarifbeschäftigten muss die Möglichkeit der Zahlung konkurrenzfähiger Vergütungen ebenfalls geschaffen werden, z. B. durch Anpassung des Tarifvertrags für den Öffentlichen Dienst (TVöD). Die bisherige Möglichkeit, zeitlich begrenzte Zulagen zu zahlen, genügen auf Dauer nicht.

Nachwuchsförderung ist dringend notwendig, denn mit jeder digitalisierten Anlage verschwindet über die Jahre auch das Fachwissen, wie die Anlage (z. B. im Bereich Wasser und Energie) notfalls auch ohne Computersysteme betrieben werden kann. Nicht nur durch Digitalisierung, sondern auch durch Renteneintritt der alten Hasen verschwindet solche, in der Krise unschätzbar wertvolle, Fähigkeiten.

Open Source in KRITIS!

Im KRITIS-Umfeld eingesetzte Software muss grundsätzlich als Open Source bereitgestellt werden oder der Quellcode muss zumindest in treuhänderische Verwaltung gegeben werden.

Software für den Betrieb der Anlagen aus den Anlagenkategorien der BSI-KritisV von kritischen Infrastrukturen muss frei sein, oder der Quellcode in treuhänderischer Verwaltung gehalten werden, damit diese auch viele Jahre und Jahrzehnte sicher betrieben werden kann. Auch wenn der Hersteller die Software nicht mehr unterstützt oder selbst nicht mehr existiert. Dies folgt als Teil-Lösung für das Problem, dass (Hardware-)Komponenten, z. B. in Produktionsanlagen, nicht ohne weiteres ausgetauscht werden können. Dies fordern wir in Anlehnung an das vom CCC unterstützte Public Money, Public Code.[7, 8]

Für SCADA- und PLC-Systeme, die bei Kritischen Infrastrukturen angewendet werden, gibt es bereits in einer Bundestags-Drucksache

17/12541, unter einen Beschluss der Enquete Kommission für digitale Infrastruktur:

> *Der Open-Source-Weg, also das Kerckhoff-Prinzip, ist daher für Kritische Infrastrukturen ein geeigneter Weg. [...]*
>
> *Wie in der Wirtschaft üblich, sollte gerade gegenüber Herstellern von Software für bestimmte Kritische Infrastrukturen zwingend darauf geachtet werden, dass der Source Code zur Überprüfung zugänglich gemacht wird.*
>
> [9, S. 98, Abschnitt 4b)]

Regulierung, Aufsicht, Kontrolle!

Kritische Infrastruktur sollte bestenfalls nicht unter vollständiger Kontrolle der Privatwirtschaft stehen.

Für jeden KRITIS-Sektor betrachten wir als Arbeitsgruppe derzeit einzeln, wie die notwendigen Kontrollmechanismen implementiert werden könnten und welche genau notwendig sind. Grundsätzlich müssen kritische Infrastrukturen sorgsamer und ausfallsicherer betrieben und ausgebaut werden, als andere Infrastrukturen. Dies widerspricht grundsätzlich den Bestrebungen des freien Marktes. Detaillierte Regulierungen, unabhängige Kontrollinstanzen und kompetente Aufsichtsbehörden für die einzelnen Sektoren sind daher notwendig.

Wir fordern, keine Budgets für Behörden, Dienste und Agenturen bereitzustellen, um damit Sicherheitslücken für einen Hackback (neudeutsch wird dies freundlich als „aktive Cyber-Abwehr" bezeichnet), Staatstrojaner zu entwickeln oder zu kaufen.

Weiterhin müssen alle Behörden, Dienste und Agenturen verpflichtet werden, ihnen bekannt gewordene Schwachstellen über das BSI als neutrale und unabhängige Stelle an den Hersteller zu melden, denn der Bevölkerungsschutz fängt bei der Kommunikation vorhandener Schwachstellen an den Hersteller zu ihrer Behebung an.

Strikt defensive Cybersicherheitsstrategie!

Wir setzen uns ein für eine strikt defensive Cybersicherheitsstrategie[10]. Wir verurteilen den Einsatz und die Bereitstellung offensiver Wirkmittel im Cyberraum. Insbesondere kritische Infrastrukturen sind anfällig für Angriffe von Cyberkriminellen oder von Drittstaaten – egal ob feindlich gesinnt oder „Freunde". Da eine zweifelsfreie Attribution der Herkunft eines Cyberangriffs nach dem Stand der Technik ausgeschlossen ist, muss davon ausgegangen werden, das sowohl der Angriff wie auch ein Gegenangriff immer auch zivile Infrastruktur treffen kann. Dies ist laut den Zusatzprotokollen der Genfer Konvention von 1977 klar ausgeschlossen [vgl. Art. 52 und 54 ZP I 11]. Auch die deutlich ältere Haager Landkriegsordnung untersagt Angriffe auf zivile Infrastruktur im weiteren Sinne.

Wir fordern daher ein internationales Abkommen, dass jegliche offensive Wirkmittel im digitalen Raum als Digitalwaffen (D-Waffen) einstuft und diese im Rahmen eines Sperrvertrags international verbietet, ähnlich wie die vorhandenen ABC-Waffensperrverträge. Im Idealfall kann man dann zukünftig nur noch von ABCD-Waffensperrverträgen sprechen.

Weiterhin sind wir der Meinung, dass Deutschland mit gutem Beispiel vorangehen muss und solche Waffen weder entwickeln noch einsetzen darf. Die geplanten Gesetzesänderungen zum Einsatz offensiver Wirkmittel im Cyberraum, an denen das BMI arbeitet, dürfen nicht durchgeführt werden.

Wir erkennen an, dass wir unsere (Kritische) Infrastrukturen bisher nicht ausreichend schützen und fordern daher, alle informationstechnischen Systeme mit dem Gedanken „Security by Design" zu gestaltet. Dies schützt proaktiv gegen erfolgreiche Angriffe aus dem Cyberraum. Alle Programmierer und Administratoren müssen konstant weitergebildet werden, was der aktuelle Stand der Technik ist. Dies gilt nicht nur im Bereich des Betriebs sondern auch in der Entwicklung und der Gestaltung sicherer Systeme. Dazu fordern wir die Einrichtung mehrerer Lehrstühle zur defensiven IT-Sicherheitsforschung und -Lehre.

Übersicht über Akronyme

- ADIV: Agentur für Innovation in der Cybersicherheit
- BaFin: Bundesanstalt für Finanzdienstleistungsaufsicht
- BBK: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- BfV: Bundesamt für Verfassungsschutz
- BKA: Bundeskriminalamt
- BMI: Bundesministerium des Innern, für Bau und Heimat
- BMVg: Bundesministerium der Verteidigung
- BND: Bundesnachrichtendienst
- BNetzA: Bundesnetzagentur
- BSI: Bundesamt für Sicherheit in der Informationstechnik
- CODE: Forschungsinstitut Cyber Defence der Universität der Bundeswehr München
- IoT: Internet of Things
- PLC: Programmable Logic Controller
- SCADA: Supervisory Control and Data Acquisition
- THW: Technisches Hilfswerk
- ZITIS: Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Referenzen

[1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG): https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[2] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV): https://www.gesetze-im-internet.de/bsi-kritisv/

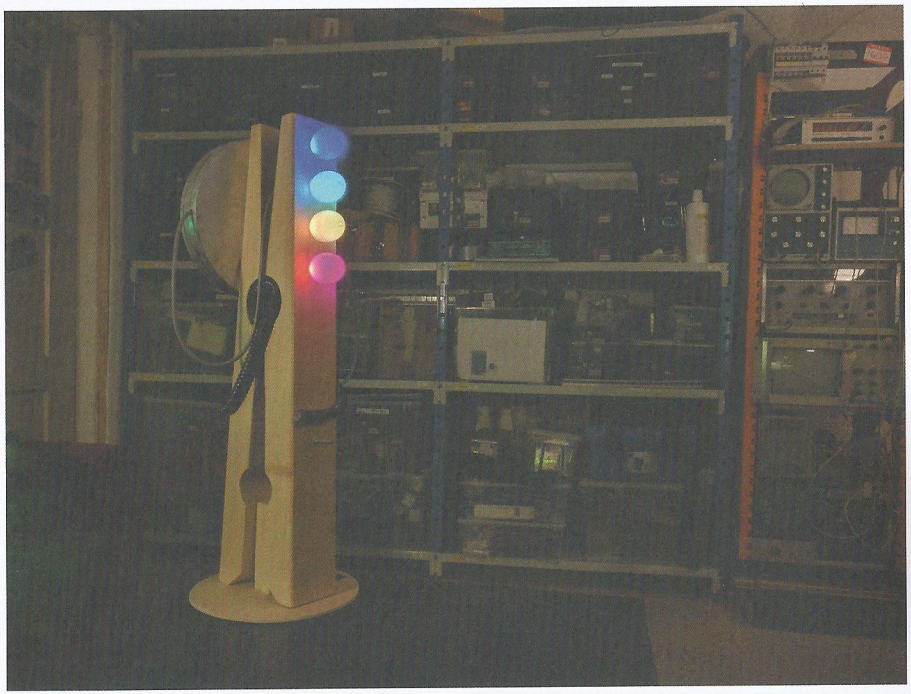
[3] 46halbe: „PC-Wahl – Open-Source-Spende: CCC schließt größte Schwachstelle in PC-Wahl" (18.09.2017), https://www.ccc.de/de/updates/2017/pc-wahl-again

[4] Presseteam des CCC: „Chaos Computer Club analysiert aktuelle Version des Staatstrojaners" (26.10.2011), https://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner

[5] Checkliste des BBK: https://www.bbk.bund.de/DE/Ratgeber/VorsorgefuerdenKatfall/Checkliste/Checkliste.html

[6] BSI: „BSI Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Abs. 2 BSIG" (2017), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientier

ungshilfe_1_0.pdf?__blob=publicationFile
[7] 46halbe: „Offener Brief: Public Money? Public Code!“ (12.09.2017), https://www.ccc.de/de/updates/2017/public-money-public-code
[8] Projekt Public Money, Public Code: https://publiccode.eu/de/
[9] Neunter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft“ http://dipbt.bundestag.de/doc/btd/17/125/1712541.pdf
[10] Erdgeist: „Chaos Computer Club fordert strikt defensive Cyber-Sicherheitsstrategie“ (29.08.2018), https://www.ccc.de/de/updates/2018/defensive-cyber-strategie
[11] Wikipedia, Zusatzprotokolle der Genfer Konvention von 1977 https://de.wikipedia.org/wiki/Genfer_Konventionen#Zusatzprotokolle_von_1977
[12] Bildquelle: CC-BY-SA 2.0 https://www.flickr.com/photos/dougbeckers/33520117275



Clemens Grünewald

Leserbriefe

Hallo liebes Team, wie mir zu meinem Erschrecken und großem Bedauern erfahren musste (und von selber hätte merken müssen!), ist das Foto auf der aktuellen DS-Ausgabe nicht von mir, sondern von Henning Hahn (@Schmierwurst, Mail siehe CC).

Henning hat mir zu Recht schon den Kopf abgerissen und ich habe vollkorn bereits informiert.

Bitte stellt in der Online-Ausgabe sicher, dass dort die richtigen Credits stehen und vollkorn sagte mir schon, dass er sich über einen „Leserbrief / Klarstellung“ von Henning freuen würde. Ich bin mir sicher ihr findet da zusammen eine Lösung.

Es tut mir sehr Leid, dass ihr unter meiner Verpeilung leiden müsst, ich hätte das ganz klar besser prüfen und meinem Verpeilerhirn misstrauen müssen (Henning hatte mir das Bild in nem Threema-Chat geschickt und von dort hat es den Weg in „meine Fotos“ gefunden :(und es wurde noch nie ein Foto von mir veröffentlicht und ich hätte mal eine Minute länger darüber nachdenken sollen, was es bedeutet ein Foto auf dem DS Cover zu veröffentlichen ...). Besonders Leid tut es mir natürlich für Henning, aber ich hoffe durch Richtigstellung und Namensnennung in der Online-Ausgabe wird wenigstens etwas Gerechtigkeit wiederhergestellt.

Ich geh mal in die Ecke mich schämen.

Liebe Grüße
<lasse>

Hi Henning, Natürlich werden wir das in der DS100, die dieses Jahr erscheint, gut sichtbar korrigieren – bitte nimm auch von uns eine Entschuldigung an, dass so etwas passieren konnte.

Viele Grüße
<rixx>

Moin rixx, danke für Deine Mail und sorry für meine verspätete Antwort.

Wenn Ihr das in der noch ausstehenden Online-Ausgabe der DS99 korrigieren könntet und, wie Du vorschlägst, in der DS100 gut sichtbar eine Gegendarstellung bringt, dann bin ich als Urheberrechtsverletzter doch weitestgehend besänftigt und werde von weiteren Schritten absehen.

Allerdings lasse ich mir noch offen, bei günstiger Gelegenheit von besagtem Hr. Lasse mein Lebendgewicht in feinstem Tschunk und/oder reinstem Bier aufwiegen zu lassen!

Grüße
<Henning>

Hallo liebe Datenschleuder-Redaktion, Sehr verehrte CCC-Mitglieder, in der aktuell heiklen Urheberrechtsreform und ihrer offenen Fragen ließ mich eine konkrete Aussage nicht mehr los: In Zukunft soll es möglich sein einen urheberrechtlichen Anspruch auf beliebige Drei-Wort-Kombinationen zu erheben. Zu diesem Zweck kam mir die Idee eines kubischen Duden. In ihm würden alle Drei-Wort-Kombinationen der deutschen Sprache enthalten sein und so künftig eine Inanspruchnahme der Urheberrechtsreform, zumindest in diesem speziellen Fall, verhindert werden.

Realisierbar wäre ein solcher Duden[3] indem eine Datenbank alle Duden-Wörter erfasst, diese pro Datensatz um eine Datenbank aller Duden-Wörter erweitert, deren Datensät-