

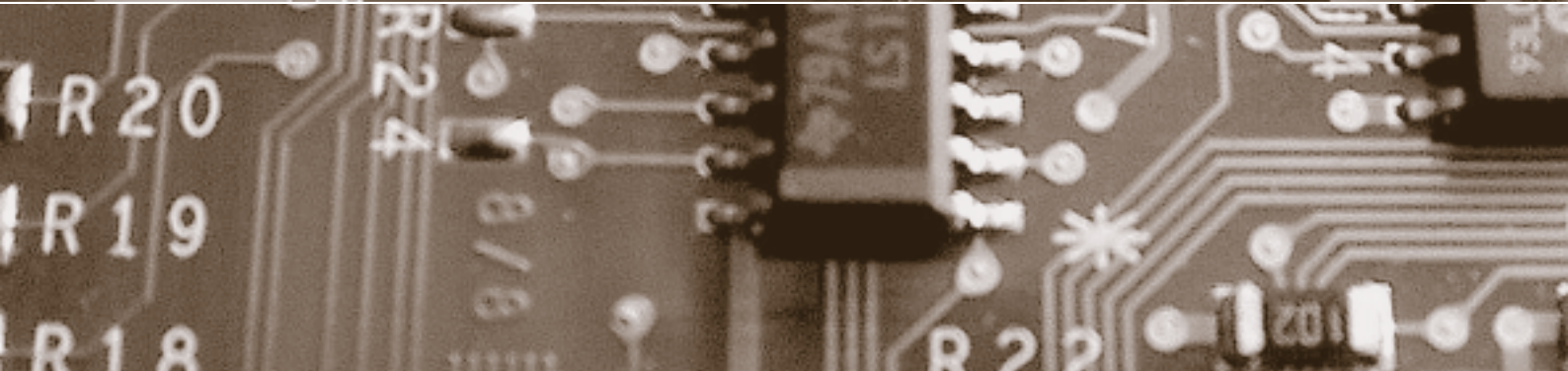
Schwerpunkt:

# Anonymisierung

**fokus:** Das Recht auf Anonymität

**fokus:** Sind anonymisierte Daten anonym genug?

**report:** Drahtlose Sensornetze – eine Herausforderung



Herausgegeben von  
**Bruno Baeriswyl**  
**Beat Rudin**  
**Bernhard M. Hämmerli**  
**Rainer J. Schweizer**  
**Günter Karjoth**

## fokus



Schwerpunkt:

### Anonymisierung

auftakt

Das Recht, in Ruhe gelassen zu werden  
von Hans-Rudolf Merz

**Seite 1**

Der Schatten über der Anonymität  
von Bruno Baeriswyl

**Seite 4**

Das Recht auf Anonymität  
von Beat Rudin

**Seite 6**

zwischenakt

Der kleine Trick mit der Angst  
von Urs Buess

**Seite 13**

Anonymisierung von genetischen Daten?  
von Bruno Baeriswyl

**Seite 14**

Sind anonymisierte Daten anonym genug?  
von Günter Karjoth

**Seite 18**

Anonymes E-Voting – eine Illusion?  
von Rolf Oppliger

**Seite 24**

Folgerungskontrolle zum Schutz  
von Information  
von Joachim Biskup

**Seite 28**

Das Recht auf Anonymität ist ein Teil des Grundrechts auf informationelle Selbstbestimmung. In der Gesetzgebung finden wir etliche Gewährleistungen. Doch auch ausserhalb dieser Bereiche könnten mit Anonymisierungs- oder Pseudonymisierungslösungen in vielen Fällen die verfolgten Zwecke erreicht werden.

### Das Recht auf Anonymität

Anonymisierung verhindert die Verletzung von Persönlichkeitsrechten. Ist das eine Lösung im Zusammenhang mit Biobanken? Jegliche Verwendung von Daten in einer Biobank setzt eine angemessene Aufklärung voraus.

### Anonymisierung von genetischen Daten?

Wann reicht eine Anonymisierung aus, damit aus den anonymisierten Daten nicht doch wieder auf die betroffenen Personen zurückgeschlossen werden kann – und die Daten für den Forschungszweck trotzdem noch aussagekräftig genug sind?

### Sind anonymisierte Daten anonym genug?

In der Theorie kann anonymes E-Voting mit Hilfe von blinden Signaturen relativ einfach realisiert werden. In der Praxis muss bei einer konkreten Realisierung eines E-Voting-Systems insbesondere darauf geachtet werden, dass nicht über verdeckte Kanäle Informationen über stimmberechtigte Personen z. B. in Tokens hineincodiert werden können.

### Anonymes E-Voting – eine Illusion?

## impresum

**digma:** Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: [www.digma.info](http://www.digma.info)

**Herausgeber:** Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

**Redaktion:** Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

**Rubrikenredaktor:** Dr. iur. Amédéo Wermelinger

**Zustelladresse:** Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel  
Tel. +41 (0)61 270 17 70, [redaktion@digma.info](mailto:redaktion@digma.info)

**Erscheinungsplan:** jeweils im März, Juni, September und Dezember

**Abonnementspreise:** Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

**Anzeigenmarketing:** Publimag AG, Europastrasse 30, Postfach, CH-8152 Glattbrugg  
Tel. +41 (0)44 809 31 11, Fax +41 (0)44 809 32 22, [www.publimag.ch](http://www.publimag.ch), [info@publimag.ch](mailto:info@publimag.ch)

**Herstellung:** Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

**Verlag und Abonnementsverwaltung:** Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich  
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, [www.schulthess.com](http://www.schulthess.com), [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

**Die Crux der  
Auskunft über  
Verstorbene**

Die Verordnungsregelung zur Herausgabe von Daten an die Angehörigen von Verstorbenen ist anspruchsvoll, weil sie eine Interessenabwägung voraussetzt. Unter welchen Voraussetzungen ist ein Privatversicherer zur Auskunft an die Angehörigen berechtigt? Wann besteht eine Pflicht dazu?

**Datenschutz und  
wirtschaftliche  
Realität**

Unter welchen Voraussetzungen kann die Wirtschaft Datenschutz realistischerweise umsetzen? Der Diskussionsbeitrag aus dem Kreis des Vereins Unternehmens-Datenschutz fordert mehr Anreize (z. B. Steuererleichterungen) für erwiesenermaßen datenschutzkonform handelnde Unternehmen. Steuererleichterung für die Einhaltung von Gesetzen – eine aus Sicht der Redaktion etwas realitätsfremde Forderung.

**Drahtlose Sensor-  
netze – eine  
Herausforderung**

Drahtlose Sensornetze werden als die nächste Technologiewelle nach RFID gehandelt. Dabei offenbaren die im Beitrag erörterten Anwendungsfelder, dass es ratsam ist, datenschutzrechtliche, aber auch ethische Fragestellungen frühzeitig zu erörtern.

**Europarechtliche  
Herausforde-  
rungen**

Bund und Kantone stehen zurzeit im Evaluationsverfahren der EU im Hinblick auf die Assoziation der Schweiz an Schengen/Dublin. Passend dazu ist ein Buch erschienen, das umfassend die europarechtlichen Vorgaben darstellt, nach denen sich das schweizerische Datenschutzrecht künftig zu richten hat.

**report**



RECHT IN DER PRAXIS  
Die Crux der Auskunft über Verstorbene  
von Martin Hofer **Seite 34**

BETRUGSPRÄVENTION  
Fraud Management: Kampf dem IT-Betrug  
von Stefan Nöpflin **Seite 40**

RECHT UND PRAXIS  
Datenschutz und wirtschaftliche Realität  
von Esther Hefti  
und Susanne Amrein-Fischer **Seite 42**

IT-SICHERHEIT  
Unterwegs im World Wild Web  
von Thomas Dübendorfer **Seite 46**

FORSCHUNG  
Drahtlose Sensornetze – eine Herausforderung  
von Dirk Westhoff  
und Heinrich Stüttgen **Seite 48**

RECHTSPRECHUNG  
Vertrauensarzt bis-repetitas  
von Amédéo Wermelinger **Seite 50**

TRANSFER  
Wie ist die Lage in der Informationssicherheit?  
von Roland Portmann **Seite 52**

**forum**



BUCHBESPRECHUNG  
Europarechtliche Herausforderungen  
von Beat Rudin **Seite 54**

agenda **Seite 55**

schlussakt  
Wo sind die Liberalen in der Schweiz?  
von Beat Rudin **Seite 56**

Cartoon  
von Hanspeter Wyss

## Internet Security

# Unterwegs im World Wild Web



Dr. Thomas Dübendorfer, Präsident der Information Security Society Switzerland ISSS  
thomas.duebendorfer@issss.ch

Stellen Sie sich vor, Sie befänden sich im Wilden Westen und würden mit der Kutsche durch die weiten Steppen reisen, um neue Orte zu entdecken. Natürlich sind Sie daran interessiert, wohlbehalten wieder zu Ihrem Ausgangsort zurückzukommen. Nun haben sich aber in letzter Zeit die Überfälle auf Kutschen merklich gehäuft. Ganz im Gegensatz zu früheren brutalen Raubüberfällen waren die aktuellen allerdings ganz subtil und ohne merkliche Gewalt. Die Bestohlenen waren sich paradoxerweise oft gar nicht bewusst, dass sie auf ihrer Reise Opfer eines Überfalls geworden waren. Erst als sie wieder von ihrer Reise zurück waren, stellten die Opfer fest, dass sich ihre Pferde irgendwie anders verhielten als sonst, beinahe als würden sie einem anderen Kutscher gehorchen. Zudem gelangten immer wieder persönliche Informationen in falsche Hände, als würden die Pferde den geheimen Diskussionen in der Kutsche lauschen. Der Kutschenhändler sagte, es sei bekannt, dass dies bei gewissen alten Kutschenmodellen häufiger passiere als bei neuen, und rät, nur noch mit dem jeweils neuesten

Kutschenmodell auf Reisen zu gehen.

## Unerwünschte Drive-By Downloads

Nun befinden wir uns nicht im Wilden Westen, sondern im World Wide Web. Sie verwenden einen Webbrowser und surfen im weiten Ozean des Internets nach Informationen. Dabei kann es passieren, dass Sie auf einer der inzwischen über drei Millionen<sup>1</sup> von Google als böse identifizierten Webseiten-URLs landen. Mehr als zwei Drittel davon befinden sich auf Webservern in China. Diese Webseiten nutzen eine Schwachstelle im Browser aus und führen unbemerkt einen sogenannten Drive-By Download aus. Sie erhalten keine Warnung, müssen keinen Pop-up-Dialog wegklicken und merken auch sonst wenig davon, dass soeben im Hintergrund ein böses Programm auf Ihrem Computer installiert wurde. Häufig handelt es sich dabei um Trojaner, die geheime Informationen ausspähen, sammeln und ins Internet senden. Etwas seltener handelt es sich aber auch um Adware, welche auf dem Desktop von nun an Werbungen einblendet. Wie konnte es zu einer derart hohen Zahl von bösen Webseiten kommen?

## Inhalte ausser Kontrolle

Im Zeitalter statischer Webseiten war der volle Inhalt einer Webseite noch unter der Kontrolle des Autors, der oft auch zugleich Webmaster war. Um

Fremdinhalte einzuschleusen, musste der Webserver gehackt oder das Passwort zum FTP-Server erspäht werden. Heute hingegen, im Zeitalter interaktiver und dynamischer Webapplikationen, hat der Webmaster oft nicht mehr die volle Kontrolle über den Inhalt seiner Webseiten – oft ohne sich dessen voll bewusst zu sein. Es gibt eine grosse und verlockende Auswahl an Fremdinhalten:

- Benutzerbeiträge in Foren;
- Widgets wie z.B. Seitenabrufzähler;
- Werbung mit Weiterverkauf des Werbeplatzes (Syndication);
- Mash-Ups z.B. mit Google Maps oder Flickr;
- fremd gehostete Videos;
- dynamische Templates insbesondere in Content Management Systemen;
- kostenlose Scripts zur Installation auf dem eigenen Webserver.

## Lieblingsblog greift an

Durch das Einbinden kann die Attraktivität der Webseite gesteigert und in einigen Fällen wie bei der Werbung auch Geld verdient werden. Das Problem mit Fremdinhalten ist, dass man dadurch die Kontrolle über einen Teil der eigenen Website an Dritte abgibt. Es ist daher entscheidend, dass der Webmaster allen gewählten Anbietern von Fremdinhalten vertrauen kann bzw. entsprechende Vorkehrungen trifft, um den Fremdinhalt auf möglichen Schadcode zu überprüfen, bevor dieser in die eigene Website

## Links

- <sup>1</sup> Google Tech Report «All Your iFRAMES Point to Us», N. PROVOs et al., Februar 2008, <<http://research.google.com/archive/provos-2008a.pdf>> (18.02.2008).
- <sup>2</sup> Secunia Blog «1 in 5 applications are not patched!», December 2007, <<http://secunia.com/blog/17/>> (18.02.2008).

aufgenommen wird. Wird dies unterlassen, kann sich sogar der eigene Blog über Nacht in eine bösartige Website verwandeln, weil z. B. der eingebundene Seitenabrufzähler neben dem Zählen der Besucher auch noch Schadcode in die Website injiziert. Dies ist u.a. bei einem populären russischen Seitenzähler passiert, der nach etlichen Jahren tadellosen Funktionierens ab 2006 plötzlich die Microsoft VM Schwachstelle MS03-11 in Internet Explorer ausnützte, um beliebigen Programmcode auf dem Rechner des Benutzers auszuführen.

Kostenlose Scripts zur Installation auf dem eigenen Webserver haben leider neben vielen tollen Features teilweise auch gravierende Sicherheitslücken (wie z. B. bei phpBB2 oder InvisionBoard), da sie zu wenig sorgfältig entwickelt und getestet wurden.

### **Scheinsicherheit**

Wer glaubt, dass das Einbinden von Fremdinhalten in einem «iframe» aufgrund der «same origin»-Sicherheitspolicy sicher sei, täuscht sich. Diese Policy schränkt zwar den Datenaustausch zwischen Scripts von verschiedenen Domains im Browser stark ein, für einen Drive-By Download genügt es allerdings bereits, wenn in einem einzigen eingebundenen iframe Schadcode enthalten ist. Das iframe muss dazu nicht einmal sichtbar sein (oft 1x1 Pixel klein oder auf unsichtbar gesetzt).

### **Vertrauen ist nicht transitiv**

Bei der Einbindung von Werbung sollte sichergestellt werden, dass der Werbewermittler die Werbebotschaften auf Qualität und Sicherheit überprüft, bevor diese freigeschaltet werden, wie dies bei grossen Werbewermittlern üb-

lich ist. Bei gewissen Werbenetzwerktypen kann der Werbekunde seinen Werbeplatz weiterverkaufen (sogenannte Syndication). Dies kann über mehrere Zwischenhändler erfolgen. In einem belegten Fall wurde ein solches javascript-basiertes Werbesystem ausgenutzt, um Schadcode über vierfach weiterverkauften Werbeplatz zu verteilen. Nur weil man dem ersten Anbieter in der Kette vertraut, heisst das noch lange nicht, dass man auch dem in vierter Indirektion vertrauen kann.

### **Sicherer Surfen**

Wer immer mit der neuesten Browserversion, aktuellem Virens scanner und aktivierter Firewall unterwegs ist, kann bereits viele Angriffe abwehren. Leider wird heute noch oft mit Patches zugewartet. Laut einer Studie<sup>2</sup> von Secunia über 14,5 Millionen Applikationen auf Enduser-Rechnern waren ganze 20% davon nicht auf dem neuesten Stand und wiesen bekannte Sicherheitslecks auf. Wer auf ActiveX, Javascript, VBScript und Plugins verzichten kann und diese deaktiviert, erhöht die Sicherheit wesentlich, kann aber gewisse Webseiten nicht mehr korrekt anzeigen.

Wird die Webseiten-URL bei Google eingetippt, enthalten die Suchresultate den Warnhinweis «Diese Website kann Ihren Computer beschädigen», sofern die angefragte Website als bösartig identifiziert wurde.

Zuletzt sollte man Symptome wie plötzliches Verlangsamten des Rechners, ungewöhnlicher Netzwerkverkehr oder häufige Abstürze zum Anlass nehmen, aktiv nach Trojanern zu suchen, am besten mit einem Scan ab bootfähiger Sicherheitscheck-CD-ROM. ■

### **Kurz & bündig**

Auch wenn das Einbinden von Fremdinhalten in eigene Webseiten sehr verlockend sein mag, sollte immer erst die Vertrauenswürdigkeit des Anbieters überprüft werden. Ansonsten zählt die eigene Webseite möglicherweise schon bald zu den mehr als drei Millionen Webseiten-URLs, welche auf den Rechnern ihrer Besucher mit einem unauffälligen Drive-by Download durch Ausnutzen einer Schwachstelle im Webbrowser Trojaner oder Adware installieren.

## Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)  
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name \_\_\_\_\_ Vorname \_\_\_\_\_

Firma \_\_\_\_\_

Strasse \_\_\_\_\_

PLZ \_\_\_\_\_ Ort \_\_\_\_\_ Land \_\_\_\_\_

Datum \_\_\_\_\_ Unterschrift \_\_\_\_\_

### Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

Homepage: [www.schulthess.com](http://www.schulthess.com)

Schulthess 