Zeitschrift für Datenrecht und Informationssicherheit

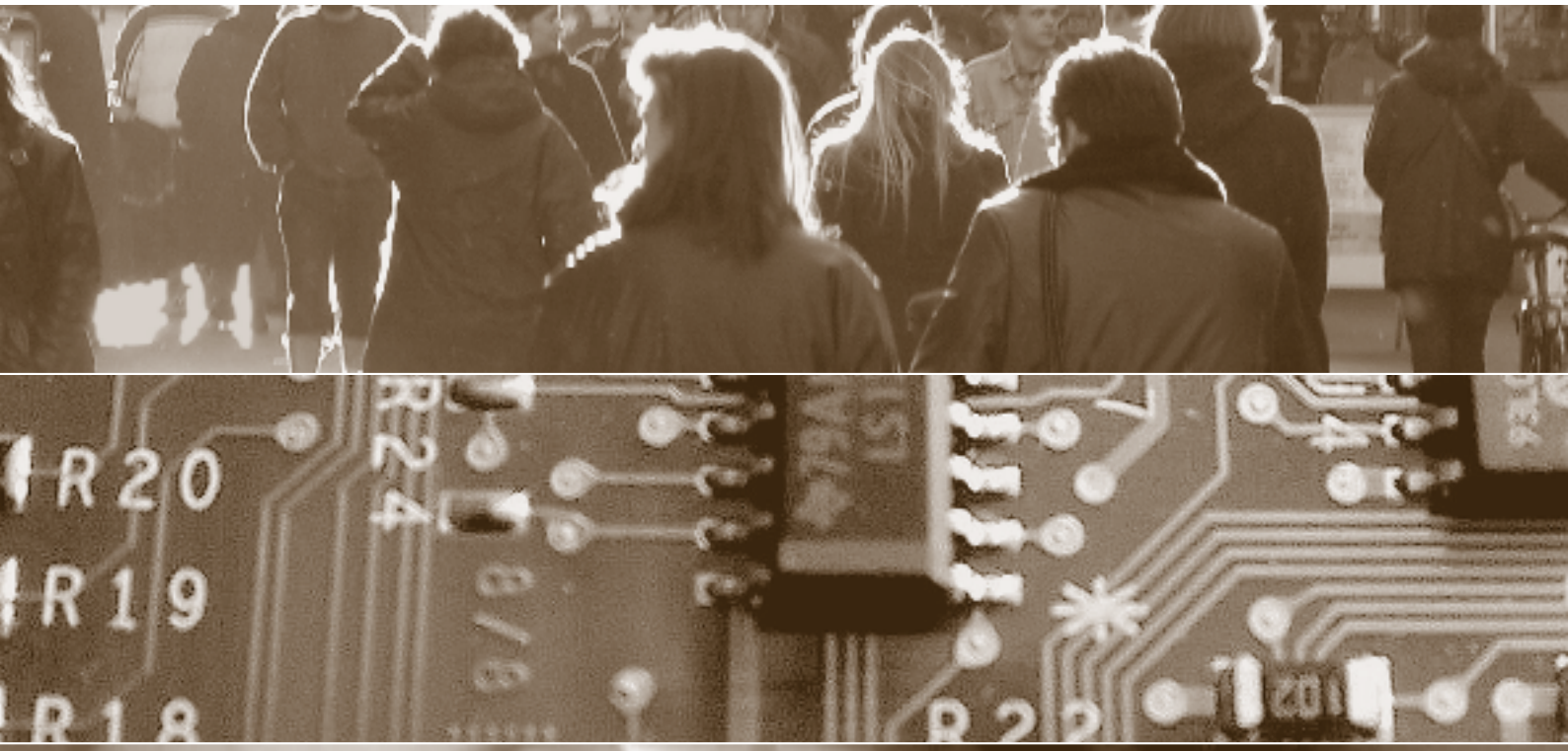
digma

www.digma.info 11. Jahrgang, Heft 3, September 2011

Schwerpunkt:

Reputation im Internet

fokus: Der Ruf nach einem Recht auf Vergessen
fokus: Rufmord im Internet bedroht Unternehmen
report: Datenschutzaspekte smarter Überwachung



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

Schulthess §

fokus

Schwerpunkt:
Reputation im Internet

Der Ruf nach einem Recht auf Vergessen

Das auf europäischer Ebene postulierte «Recht auf Vergessen» will dem Einzelnen das Recht einräumen, Daten auf dem Internet «zum Verschwinden» zu bringen. Die gegenwärtige Diskussion erweist sich aber noch als zu vage: Die Schaffung eines neuen Grundrechts allein genügt nicht; ein neues Grundrecht erfordert die konkrete Umsetzung in ein spezifisches Anspruchssystem.

Nutzen und Risiken von Internetreputation

Bewertungssysteme im Internet sind hilfreich – sie können aber auch missbraucht werden. Es sind deshalb datenschutzfreundliche Designoptionen für Reputationssysteme zu entwickeln, die sowohl die Integrität der Informationen als auch die datenschutzrechtlichen Anforderungen erfüllen. Die Autorin plädiert deshalb für die Verknüpfung solcher Systeme mit Identitätsmanagementsystemen.

Rufmord im Internet bedroht Unternehmen

Rufmord im Internet betrifft nicht allein Facebook-Anwender: Blogs, Bewertungsportale und soziale Netzwerke können auch Firmen in existenzielle Krisen stürzen. Jeder kann Opfer werden – jeder kann Täter werden. Was kann man dagegen unternehmen?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: 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

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien 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, zs.verlag@schulthess.com

Skimming – Tatphasen und Haftung

Das Skimming ist zu einem einträglichen Geschäft geworden. Weil sich die Formen, in denen sich die Kriminellen der Informationstechnik und des Internets bedienen, immer mehr annähern, werden sich die «klassische» und die Cyberkriminalität wegen ihrer Methoden und Vorgehensweisen kaum noch unterscheiden. Die deutsche Rechtsprechung hatte sich schon mit Skimming zu befassen.

Datenschutzaspekte smarter Überwachung

Moderne «intelligente» Überwachungssysteme sollen den Bürger besser vor Terrorismus und organisierter Kriminalität schützen, greifen potenziell aber tief in die Privatsphäre des Einzelnen ein. Das EU-Forschungsprojekt SAPIENT untersucht die Risiken solcher intelligenten Überwachungstechniken und erarbeitet Verfahren, um diese im Einklang mit Menschenrechten und unter Beachtung des sozialen und gemeinschaftlichen Zusammenhalts gestalten zu können.

Vertrauensbildung bei Internetwahlen

Nicht nur, dass die Hacker-Gruppe «Anonymous» möglicherweise E-Voting angreifen will – E-Voting sieht sich auch sonst vielen Zweifeln gegenüber: Zweifeln am Nutzen, Zweifeln an der Sicherheit der Technologie, Zweifeln an der Nachvollziehbarkeit des Wahlprozesses, insbesondere bezüglich der Korrektheit des berechneten Wahlergebnisses. Kurz: Kann man E-Voting vertrauen? Die Autoren schlagen vertrauensbildende Massnahmen vor.

Das Risiko «Risk-Management»

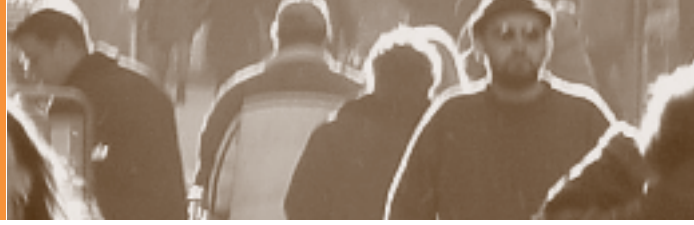
Die vorbildliche Firma führt seit Jahren ein IT-Risikomanagement. Die alten Risiken hat sie immer besser im Griff – aber kennt sie auch die neuen? Und kann sie die IT-Risiken auch bewerten? Der Autor weist aufgrund seiner Erfahrung als externer Fachexperte bei ISO/IEC 27001-Zertifizierungen auf die Risiken beim Risikomanagement hin.

Aus den Datenschutzbehörden

Wer ist neu zur Datenschutzbeauftragten gewählt worden? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die neue Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzszene.

report

forum



ISSS

SuisseID und Identitätsmissbrauch

Alexander Herrigel, Dr., Informations- und ICT-Sicherheitsspezialist im Leistungszentrum Risiko- und Prozessmanagement der Luzerner Kantonalbank, Vorstandsmitglied ISSS, Luzern alexander.herrigel@lukb.ch

Am ISSS Security Lunch vom 28. Juni 2011 in Bern informierte zuerst Marc Zweiacker, Leiter der Arbeitsgruppe Sicherheit im Trägerverein SuisseID, über die Aktivitäten der Arbeitsgruppe Sicherheit. Der Trägerverein hat aktuell vier Arbeitsgruppen mit unterschiedlichen Schwerpunkten: Spezifikation, Sicherheit, Marketing und Internationales. Aufgrund der Berichte und Erfahrungen im letzten Jahr beschäftigt sich die Arbeitsgruppe Sicherheit mit einer szenariobasierten Risikoanalyse zum SuisseID-Missbrauch. Basierend auf einem zurzeit durch das Bundesamt für Justiz in Arbeit befindlichen Rechtsgutachten und auf einer technischen Studie betreffend Eintretenswahrscheinlichkeit von allfälligen Missbräuchen werden die Ergebnisse per Ende Jahr vorliegen. Erstmals wird über den Stand Ende August in einer Info-Veranstaltung orientiert.

Als nächster Redner berichtete Fredy Schwyter, als Vertreter von Anthony Thorn, über die Ergebnisse der ISSS Special Interest Group «SuisseID – benefits and risks for e-Commerce», welche die folgenden Sachverhalte diskutierte:

- Der Inhaber eines Signaturschlüssels haftet einer Drittperson und muss dieser einen angemessenen Schadenersatz für den verursachten Schaden bezahlen. Was bedeutet dies, wenn jemand im Namen seines Arbeitgebers handelt?
- Die Haftung für den Schadenersatz entfällt, wenn nachgewiesen werden kann, dass notwendige und zumutbare Sicherheitsvorkehrungen getroffen worden sind. Der Bundesrat hat aber bis heute die notwendigen Sicherheitsvorkehrungen nicht bestimmt. Es ist daher unklar, was notwendig und zumutbar bedeutet.
- Die gemeinsame Verwendung des IAC für die Authentisierung und des QC für die Nichtabstreitbarkeit wird infrage gestellt. Wegen der vorgetragenen Kritikpunkte wurde empfohlen, einen Kartenleser, der mit der Sicherheitsklasse 2 zertifiziert wurde, einzusetzen und jeweils sorgfältig abzuwägen, ob die möglichen Bedrohungen das Risiko rechtfertigen.

Danach stellte Gunnar Porada den Einsatz der SuisseID prinzipiell infrage, in dem er zeigte, wie er mit einem Trojaner-Programm die SuisseID eines Teilnehmers der Veranstaltung zweckentfremden und in seinem Namen rechtsverbindliche Tätigkeiten bei <http://www.cashare.ch/> durchführen kann. Herr Porada stellte die Frage nach einem möglichen Schutz des SuisseID-Anwenders im Missbrauchsfall, der trotz aller Antivirenprogramme und persönlichen Firewalls möglich ist. «Wenn Sie ihre eigene Unschuld nicht beweisen können», wie können Sie bei einer rechtsverbindlichen Unterschrift (digitale Signatur) beweisen, dass Sie nicht für den Schaden aufkommen müssen?

Samuel Klaus diskutierte anschliessend die rechtlichen Risiken und Haftungsfragen, die bei einer missbräuchlichen Verwendung der SuisseID auftreten können, und verwies hierbei darauf, dass die Signaturerstellungseinheiten gewährleisten müssen, dass die für die Erzeugung der Signatur verwendeten Signaturschlüssel vor der missbräuchlichen Verwendung durch andere Personen verlässlich geschützt werden. Der Zertifizierungsdienstanbieter hat daher zu überprüfen, ob der Schlüsselhalter über eine sichere Signatureinheit verfügt. Der zu Schaden gekommene Endanwender der SuisseID hat daher prinzipiell das Recht, den Zertifizierungsdienste-Anbieter mit Regressansprüchen zu konfrontieren. Da es aber noch keine Gerichtspraxis gibt, ist offen, ob sich der Endanwender gegen einen missbräuchlich signierten Vertrag wirklich wehren kann oder nicht. ■

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (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
Homepage: www.schulthess.com

Schulthess §