Zeitschrift für Datenrecht und Informationssicherheit

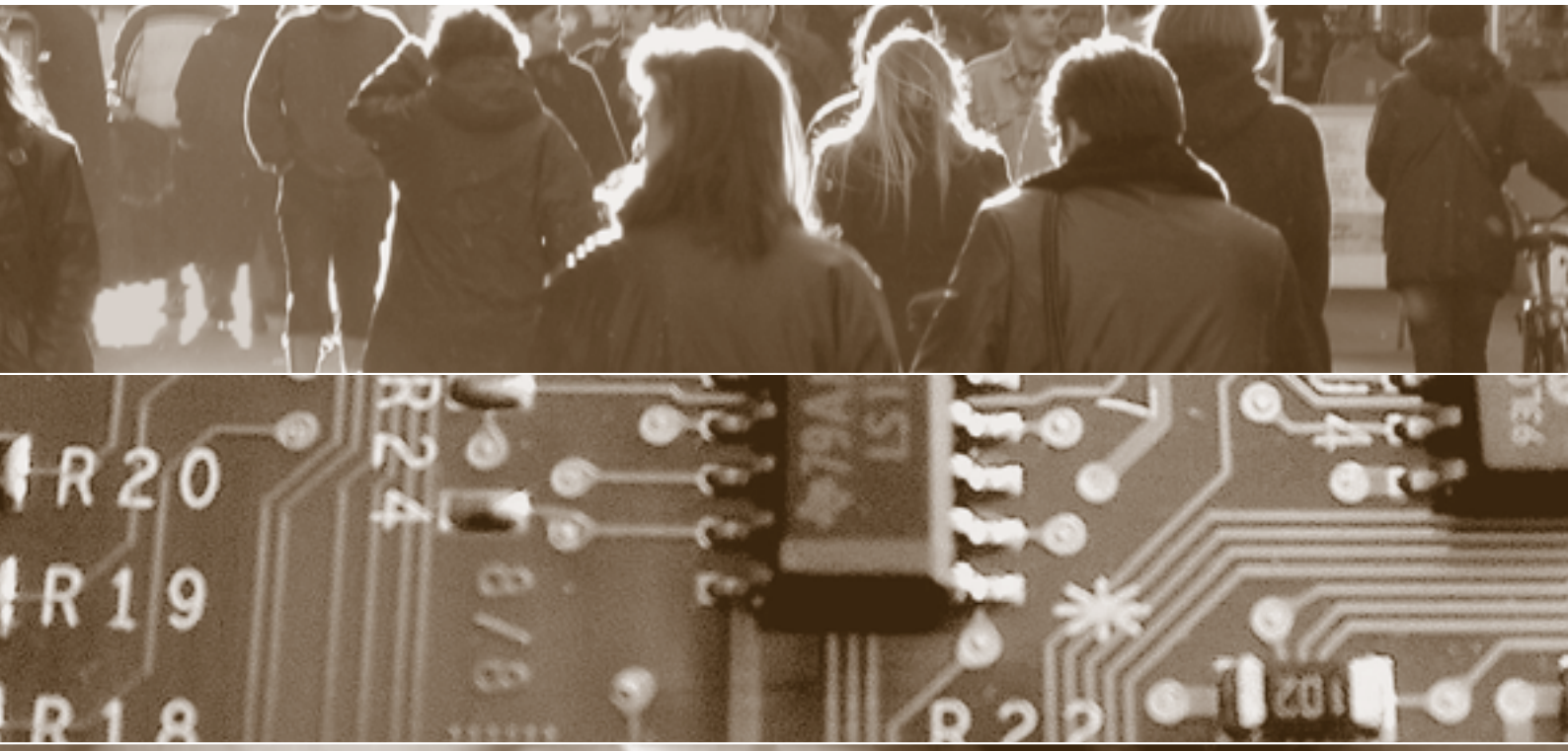
digma

www.digma.info 12. Jahrgang, Heft 1, April 2012

Schwerpunkt:

Sensor-Actor-Netze

fokus: Lagebild für Kritische Infrastrukturen
fokus: Privatsphäre trotz intelligenter Zähler
report: Sicherheit im Cloud Computing



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

Schulthess §

inhalt

fokus

Schwerpunkt:
Sensor-Actor-Netze

Lagebild für Kritische Infrastrukturen

Für den Schutz Kritischer Infrastrukturen (SKI) ist der regelmässige Austausch von Informationen zwischen Behörden und Unternehmen unerlässlich. Dieser könnte in einem SKI-relevanten Lagebild gebündelt und aufbereitet werden. Darin können Behörden und Betreiber Informationen zum Schutz Kritischer Infrastrukturen bündeln und die Koordination im Hinblick auf Schutzmassnahmen verbessern.

Sicherheit im Energienetz der Zukunft

Durch den vermehrten Einsatz von ICT und der damit verbundenen erhöhten Anzahl von Schnittstellen im Energienetz entstehen neue Sicherheitsrisiken in Bezug auf Netzverfügbarkeit, Systemintegrität und Datenschutz. Ein Sicherheitskonzept für das intelligente Stromnetz der Zukunft sollte frühzeitig geplant werden.

PET – ein Konzept harrt der Umsetzung

Mit «Privacy Enhancing Technology» (PET) sollen neue Anwendungen «datenschutzverträglich» gemacht werden. Die inhärenten Zielkonflikte können nur aufgelöst werden, wenn neben der Technik auch das Datenschutzrecht in die Betrachtung einbezogen wird.

Privatsphäre trotz Intelligenter Zähler

Intelligente Zähler versprechen eine bessere Ausnutzung vorhandener Infrastruktur für Netzbetreiber und erhöhte Transparenz für Konsumenten. Kann die Privatsphäre im eigenen Heim bedingungslos geschützt werden, oder folgt auf den gläsernen Mobilfunkkunden nun der gläserne Stromkunde?

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 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Sicherheit im Cloud Computing

Obwohl in den Medien intensiv über Cloud Computing und entsprechende ökonomische Vorteile berichtet wird, werden die latent vorhandenen Sicherheitsprobleme meist verschwiegen bzw. ignoriert. Muss man den Cloud-Anbietern einfach vertrauen?

E-Learning: Kryptografie und -analyse

Das Open-Source-Projekt CrypTool (CT) hat sich die Aufgabe gestellt, Kryptografie und Kryptoanalyse mit Beispielen und Visualisierungen so darzustellen, dass man ein gutes Verständnis und Awareness für IT-Sicherheit erreicht.

Familie und Arbeitsplatz: heikle Ortung

Location Based Services sind heikel oder unzulässig, wenn sie der Überwachung von Kindern und Arbeitnehmenden dienen. Die gesetzliche Vertretung ist bei älteren Kindern meist nicht befugt, an deren Stelle die Einwilligung zur Datenbearbeitung zu erteilen. Das Arbeitsrecht schränkt die Überwachung von Arbeitnehmenden erheblich ein.

EU: Zu neuen Ufern lockt ein neuer Tag?

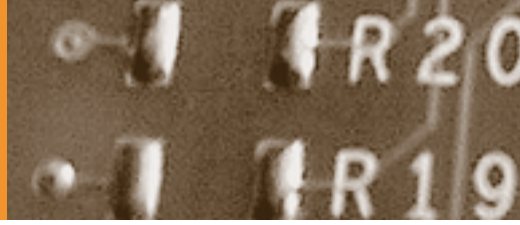
Die EU-Kommission hat Entwürfe für eine «Regulation» und eine «Directive» zur Vereinheitlichung des Datenschutzrechts vorgelegt. Mit dem darin enthaltenen «right to be forgotten» und dem Strafenkatalog würde ein bedeutender Schritt in Richtung Harmonisierung des Datenschutzrechts getan. Es ist zu hoffen, dass der Gedanke der Entwürfe in der definitiven Fassung immer noch zu erkennen sein wird.

Aus den Datenschutzbehörden

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

report

forum



Sicherheit

Sicherheit im Cloud Computing

Rolf Oppliger, Prof. Dr., Titularprofessor an der Universität Zürich und Informatiksicherheitsbeauftragter im Informatiksteuerungsorgan des Bundes ISB, Bern
rolf.oppliger@isb.admin.ch

Die einschlägige Fachpresse ist voll von Artikeln, die die Vorzüge von Cloud Computing preisen und damit suggerieren, dass es für IT-Verantwortliche kaum eine Alternative gibt. Tatsächlich gibt es sinnvolle und erfolgversprechende Einsatzmöglichkeiten und -gebiete für Cloud Computing (immer wenn es um Skalierbarkeit und Elastizität bei der IT-Leistungserbringung geht). Leider wird aber oft auch undifferenziert über diese neue Form des Outsourcing und seine vermeintlich nicht existierenden oder gelösten Sicherheitsprobleme berichtet. Insbesondere rühmen sich Anbieter mit dem Einhalten von einschlägigen Standards und Schnittstellen, damit es keinen Lock-in-Effekt gebe. Das ist aber nur die Vorderseite der Medaille. Auf der Rückseite sind weder alle Sicherheitsprobleme gelöst noch gibt es Standards und Schnittstellen, die einen Lock-in-Effekt überhaupt erst verhindern könnten.

Das Mädchen und die Cloud

Eine kleine aber wahre Geschichte soll eines der zentralen Sicherheitsprobleme von Cloud Computing verdeutlichen: Ein Mädchen hat vor ein paar Jahren ein Mailkonto bei einem grossen namhaften U.S.-amerikanischen Cloud-Anbieter eröffnet und seither rege genutzt. Aufgrund des Versprechens des Anbieters, dass die Daten in der Cloud gehalten und damit sicher und (beim Zugriff über IMAP) auch jederzeit verfügbar seien, hat das Mädchen auf das Anlegen von Sicherungskopien verzichtet. Doch eines Tages hat sich der Anbieter auf den Children's Online Privacy Protection Act (COPPA, <http://www.coppa.org>) aus dem Jahre 1998 zurückbesonnen, der für die Betreiber von Webseiten Regeln vorgibt, wie mit persönlichen Daten von Kindern unter 13 Jahren umzugehen ist. Insbesondere hat der Anbieter sein Anmeldeverfahren geändert und es für bekennende Unter-13-Jährige verunmöglicht, überhaupt erst ein Konto zu eröffnen (das Verfahren gilt für alle Dienste des Anbieters). Nachdem das Mädchen erfolglos versucht hat, sich beim sozialen Netzdienst des Anbieters anzumelden, ist es ohne Vorwarnung vom weiteren Zugriff auf sein (bestehendes) Mailkonto ausgesperrt worden. Dass Unter-13-Jährige keine neuen Konti eröffnen können, ist grundsätzlich verständlich, nachvollziehbar und sogar sinnvoll. Weshalb aber Unter-13-Jährige, die bereits über ein Konto verfügen und dieses unter Angabe ihres wahren Alters eingerichtet haben, am Zugriff auf ihre Daten gehindert werden, ist weder verständlich noch nachvollziehbar (es macht nicht einmal aus der Sicht des Anbieters Sinn). Da hilft es wenig, wenn der Anbieter den Betroffenen rät, sie (bzw. ihre Eltern) sollen sich doch unter Einsendung von Kopien von amtlichen Ausweisdokumenten an die Rechtsabteilung in den USA wenden. Ein solcher Ratschlag droht nicht nur in einen endlosen und wenig erfolgversprechenden Austausch von Nachrichten zu münden, sondern – und das ist eigentlich wichtiger – steht auch im Widerspruch zu allem, was man sonst im Hinblick auf Phishing- und andere «Social Engineering»-Angriffe aus Sicherheitsgründen empfiehlt. Dabei gäbe es eine einfache Lösung für das Problem: Der Anbieter könnte den betroffenen Kunden einen zeitlich befristeten Zugriff gewähren, damit diese ihre Daten kontrolliert exportieren und in ein anderes Mailsystem importieren könnten. So aber verbleiben die Daten im Rechenzentrum des Anbieters. Mit grosser Wahrscheinlichkeit werden die Daten sogar redundant in mehreren Rechenzentren gehalten, ohne dass der Kunde Zugriff darauf erhält. Das ist aus der Sicht des Kunden nicht nur aus datenschutzrechtlicher Sicht problematisch.

Das grundsätzliche Problem

Nun geht es bei dieser Geschichte weder um den konkreten (Einzel-) Fall noch um den Cloud-Anbieter. Stattdessen geht um das grundsätzliche Problem: Ein Anbieter irgendwo auf dieser Welt übernimmt die Daten eines Kunden. Die Übernahme verläuft solange gut, bis sich eines Tages die gesetzlichen und/oder regulatorischen Rahmenbedingungen im Heimatland des Anbieters ändern oder diese Rahmenbedingungen vom Anbieter auch nur anders interpretiert und umgesetzt werden. Dabei kann es sein, dass der Kunde Zugriff auf seine Daten verliert. Einen Lock-in-Effekt im eigentlichen Sinn gibt es zwar nicht, dafür aber einen umso fataleren Lock-out-Effekt, d.h., der Kunde wird vom Zugriff auf seine Daten ausgeschlossen. Das kann überall und jederzeit geschehen und entzieht sich der Einflussnahme durch den Kunden. Gerade die letzten Jahre haben gezeigt, wie schnell sich vor dem Hintergrund latent vorhandener Terrorbedrohungen gesetzliche und/oder regulatorische Rahmenbedingungen oder deren Interpretation und Umsetzung ändern können.

Wenn ein Kunde – wie im vorliegenden Fall – ein Mädchen ist, dann halten sich die wirtschaftlichen und anderen Folgen in Grenzen und der Kunde kann wohl oder übel mit einer Aussperrung leben. Wenn der Kunde aber ein Unternehmen ist, das den Lockrufen der Anbieter erlegen ist und seine Daten in die Cloud ausgelagert hat, dann sind die Folgen nicht nur wirtschaftlich fatal, sondern möglicherweise sogar existenzbedrohend. Insofern könnte man – zugegebenermassen etwas überspitzt – formulieren, dass Cloud Computing eine Option für Kunden darstellt, die im Ernstfall auf ihre Daten bzw. den Zugriff darauf verzichten können. Natürlich könnte ein Kunde regelmässige Sicherungskopien seiner Daten machen und entsprechende Recovery-Prozeduren einüben. Nur entspricht das nicht der ursprünglichen Idee von Cloud Computing. Zudem wäre der Aufwand so hoch, dass er in der Praxis kaum getrieben werden kann (und von den Anbietern auch nicht empfohlen wird).

Aufgrund des bisher Gesagten gibt es im Zusammenhang mit Cloud Computing primär ein Verfügbarkeitsproblem zu beachten. Wie kann sichergestellt werden, dass die ausgelagerten Daten in jedem Fall und zu jeder Zeit auch unter veränderten gesetzlichen und/oder regulatorischen Rahmenbedingungen bzw. Umsetzungen verfügbar sind? Neben einem bewussten Ausschluss gibt es dabei auch Fälle zu beachten, bei denen technische Probleme und Störungen zu einem Datenverlust führen können. Solche Fälle hat es in der noch jungen Vergangenheit von Cloud Computing auch schon gegeben, auch wenn die volkswirtschaftlichen Implikationen und die entsprechenden Schlagzeilen noch klein geblieben sind. Das Problem (und das entsprechende Risiko) ist aber latent vorhanden.

Andere Sicherheitsprobleme

Neben dem geschilderten Verfügbarkeitsproblem gibt es im Zusammenhang mit Cloud Computing auch noch andere Sicherheitsprobleme zu beachten, die die klassischen Sicherheitsziele Authentizität, Integrität und Vertraulichkeit (von Daten) betreffen. Die Anbieter verweisen hier gerne auf das technisch Machbare und geben als Beispiele meist Storage Clouds an. Bei diesen Dienstangeboten beschränkt sich der Anbieter auf das Speichern von Kundendaten. Solche Clouds können sehr einfach dadurch abgesichert werden, dass man alle Daten, die beim Anbieter gespeichert werden, vor ihrer Speicherung verschlüsselt, und nach ihrer Auslieferung vom Anbieter zum Kunden wieder entschlüsselt. Die Ver- und Entschlüsselung kann dabei transparent erfolgen, so dass der Anbieter nur verschlüsselte Daten erhält und damit nichts Sinnvolles machen kann. Die Sicherheitsprobleme scheinen in diesem Fall gelöst, wenigstens wenn der Kunde selbst um die Schlüsselverwaltung besorgt ist. Leider gibt es auch Cloud-Anbieter, die dem Kunden sogar die Schlüsselverwaltung abnehmen wollen und damit

Kurz&bündig

Obwohl in den Medien intensiv über Cloud Computing und entsprechende ökonomische Vorteile berichtet wird, werden die latent vorhandenen Sicherheitsprobleme meist verschwiegen bzw. ignoriert. Dabei gibt es sowohl auf der Seite der Verfügbarkeit als auch auf der Seite der Vertraulichkeit durchaus noch offene Fragestellungen und Probleme. Am Horizont zeichnen sich zwar erste technische Lösungsansätze ab (z.B. voll homomorphe Verschlüsselungssysteme), doch wird deren praktische Umsetzung vermutlich noch einige Zeit in Anspruch nehmen. In der Zwischenzeit wird man den Cloud-Anbietern dahingehend vertrauen müssen, dass sie mit den Datenbeständen ihrer Kunden sorgfältig und vertrauenswürdig umgehen. Ob dieses Vertrauen gerechtfertigt ist, kann nur im Einzelfall und wahrscheinlich erst retrospektiv entschieden werden.

den eigentlichen Sinn und Zweck einer Verschlüsselung infrage stellen.

Bei all diesen die Verschlüsselung betreffenden Ausführungen wird gut und gerne vergessen, dass Storage Clouds nur eine relativ uninteressante Form von Cloud Computing darstellen. Interessanter sind Formen, bei denen Cloud-Anbieter über den Daten der Kunden auch operieren bzw. mit diesen Daten Berechnungen durchführen können. Hier ist man lange Zeit davon ausgegangen, dass dazu anbieterseitig die Daten im Klartext vorliegen müssen. Doch wie so oft in der modernen Kryptografie hat sich auch hier die intuitive Vorstellung als falsch erwiesen, und sinnvolle Berechnungen über verschlüsselten Daten scheinen möglich zu sein.

Voll homomorphe Verschlüsselung

Wenn man sich die Eigenschaften gängiger (asymmetrischer) Verschlüsselungssysteme vergegenwärtigt, stellt man fest, dass einige (additiv oder multiplikativ) homomorph sind. Im Falle eines multiplikativ homomorphen Verschlüsselungssystems (z.B. RSA ohne Padding) kann man zwei Chiffrate miteinander multiplizieren und erhält damit das Chiffrat des Produktes der entsprechenden Klartexte, d.h. $E(m_1)\cdot E(m_2) = E(m_1\cdot m_2)$ für eine Verschlüsselungsfunktion E und zwei Klartexte m_1 und m_2. Damit kann man mit Chiffraten in Bezug auf die Multiplikation rechnen, ohne die entsprechenden Klartexte zu kennen. Das ist zwar oft von sicherheitstechnischem Nachteil, kann aber auch für neue Anwendungen genutzt werden (z.B. E-Voting). Für additiv homomorphe Verschlüsselungssysteme gilt Analoges. Nun wäre es interessant, über Verschlüsselungssysteme zu verfügen, die nicht nur multiplikativ oder additiv homomorph sind, sondern gleichzeitig beide Eigenschaften aufweisen (d.h. sowohl multiplikativ als auch additiv homomorph sind). Damit könnte man Chiffrate multiplizieren und addieren, ohne die entsprechenden Klartexte zu kennen. Man spricht dann von einer voll homomorphen Verschlüsselung, wohl auch deshalb, weil man mithilfe der Addition und Multiplikation fast jede Operation nachbilden kann.

Die Bedeutung von voll homomorphen Verschlüsselungssystemen wurde in der Theorie schon relativ früh – d.h. ein Jahr nach der Entdeckung von RSA – erkannt und deren Existenz wurde damals als offene Frage postuliert[1]. Die theoretisch interessante aber praktisch bis zum Aufkommen von Cloud Computing eher uninteressante Frage hat mehr als 30 Jahre auf eine Beantwortung gewartet. Erst 2009 hat Craig Gentry die Frage bejaht und ein erstes – allerdings für den praktischen Einsatz noch viel zu ineffizientes – voll homomorphes Verschlüsselungssystem vorgeschlagen[2]. Dieser Vorschlag gilt als wissenschaftlicher Durchbruch, und seither ist das Entwerfen von effizienten voll homomorphen Verschlüsselungssystemen eines der hauptsächlichen Forschungsgebiete für Kryptografen. Entsprechend darf man hoffen, dass früher oder später effiziente und praktikable Systeme gefunden werden. Bis das allerdings so weit ist, muss man einem Anbieter dahingehend vertrauen, dass er mit den Daten sorgsam und vertrauenswürdig umgeht. Ob dieses Vertrauen gerechtfertigt ist, wird die Geschichte zeigen müssen. Interessant werden Fälle sein, in denen staatliche Stellen die Herausgabe von Kundendaten erzwingen (in vielen Staaten sind die dazu erforderlichen rechtlichen Voraussetzungen gegeben). Zudem werden auch voll homomorphe Verschlüsselungssysteme nicht alle Vertraulichkeitsprobleme lösen. Man denke hier z.B. an einen Kunden, der Teile seiner Daten als Ausdruck braucht. Solche Ausdrucke werden zwingend im Klartext erstellt werden müssen.

Bankenanalogie

Anlässlich einer kürzlich durchgeführten Tagung zum Thema «Sicherheit im Cloud Computing» hat ein Referent (des aus der einleitenden Geschichte bekannten Anbieters) die Situation mit der Bankenwelt verglichen, wo wir auch über eine vergleichsweise lange Zeit gelernt haben, unser Geld Institutionen – in diesem Fall Banken – anzuvertrauen, die das Geld nicht nur «sicher» verwahren, sondern damit auch etwas Sinnvolles und möglichst Wertsteigerndes machen. Dieser Analogie folgend würde der Cloud-Anbieter nicht nur Daten «sicher» verwahren, sondern mit diesen Daten auch etwas machen, das einen gewissen Mehrwert erzeugt (z.B. zielgerichtete Werbung). Ob Kunden aber wirklich wünschen, dass mit ihren Daten etwas Wertsteigerndes gemacht wird, ist fraglich. Weiter ist unklar, wie eine Wertsteigerung bei Daten über-

Fussnoten

1 Ronald L . Rivest/Len Adleman/Michael L. Dertouzos, On data banks and privacy homomorphisms, Foundations of Secure Computation, 1978, <http://people.csail.mit.edu/rivest/RivestAdleman-Dertouzos-OnDataBanksAndPrivacyHomomorphisms.pdf>.

2 Craig Gentry, Fully Homomorphic Encryption Using Ideal Lattices, Proceedings of the 41st ACM Symposium on Theory of Computing (STOC), 2009.

haupt aussehen kann (dies natürlich im Gegensatz zu monetären Werten, wo die Bedeutung klar ist und auch gemessen werden kann). Daten haben grundsätzlich andere Eigenschaften und Anforderungen als monetäre Werte (z.B. kann man Daten im Gegensatz zu echtem Geld einfach kopieren). Natürlich muss beides «sicher» verwahrt werden, aber alles andere ist offen und muss im Einzelfall diskutiert werden. Jedenfalls hinkt die Analogie mit der Bankenwelt und sie sollte nicht im Rahmen eines Plädoyers für Cloud Computing verwendet werden.

Schlussfolgerungen und Ausblick

Was heisst das nun alles für die Praxis? Zunächst einmal sollte man sich nicht von redundanten Rechenzentren dahingehend täuschen lassen, dass die Verfügbarkeit der ausgelagerten Daten in jedem Fall gegeben ist. Gesetzliche und/oder regulatorische Rahmenbedingungen oder deren Interpretation und Umsetzung können sich (sehr schnell) ändern und mit ihnen auch allfällige Zugriffsmöglichkeiten. Hier haben Anbieter Vorteile, die im gleichen Land ansässig sind wie ihre Kunden (damit die gesetzlichen und/oder regulatorischen Rahmenbedingungen wenigstens gleich sind und Rechtstreite besser geführt werden können). Bei international aufgestellten Unternehmen wird die diesbezügliche Situation sehr schnell kompliziert und unübersichtlich. Weiter sollte man sich vergegenwärtigen, was man unter einem Cloud Computing Angebot effektiv versteht. Bei Storage Clouds sind die nicht die Verfügbarkeit betreffenden Sicherheitsprobleme grundsätzlich lösbar (obwohl der praktische Einsatz von Verschlüsselungstechnologien auch nicht trivial ist). Bei allen anderen Cloud-Angeboten (und das wird die Mehrzahl sein) sieht das Ganze schwieriger und komplizierter aus. Hier wird es auf den Einzelfall ankommen. In jedem Fall wird man hier dem Anbieter vertrauen müssen. Dabei ist «vertrauen» oft ein Synonym für «ich habe keine andere Wahl», und es ist entsprechend schwierig, Vertrauen sinnvoll zu quantifizieren. Sicherlich helfen hier Zertifizierungen (z.B. ISO/IEC 27001:2005). Dennoch kann im Einzelfall der monetäre Wert von Daten so gross sein, dass ein Cloud-Anbieter den Versuchungen erliegt, und mit den Daten etwas macht bzw. Kopien davon weiterverkauft. So etwas ist in der digitalen Welt leider ohne Spuren möglich und vom Opfer kaum erkennbar (ausser an den Folgen) und schon gar nicht beweisbar. Hier gibt es keine Zertifizierung, die davor schützen könnte.

In jedem Fall lohnt es sich, die Sicherheitsdiskussion(en) rund um Cloud Computing offen und differenziert zu führen, und die entsprechenden Versprechen der Anbieter kritisch zu hinterfragen. Wie einleitend erwähnt, geht es hier um eine spezielle Form des Outsourcing, und wenn wir etwas aus vergangenen Outsourcing-Übungen gelernt haben, dann ist es die Erkenntnis, dass das in der Praxis alles viel schwieriger ist als in der Theorie. Voll homomorphe Verschlüsselungssysteme werden zwar weiterhelfen, doch ist hier noch reichlich Grundlagen- und weiter gehende Forschungs- und Entwicklungsarbeit erforderlich. In jedem Fall lohnt es sich, sich defensiv zu verhalten, und bei der Auslagerung von Daten nicht gerade mit den für das Unternehmen wichtigsten Beständen zu beginnen. ■

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 §