Zeitschrift für Datenrecht und Informationssicherheit

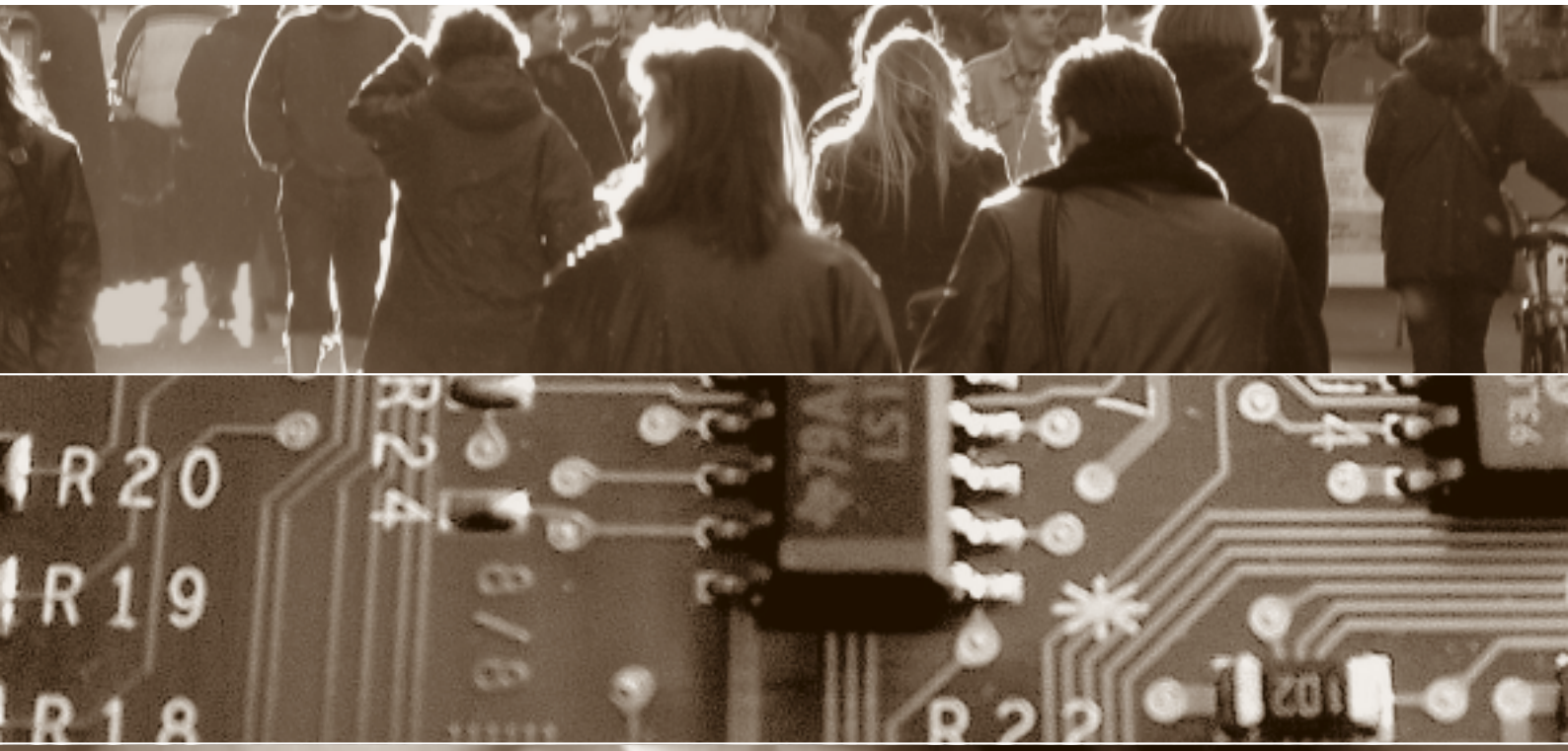
digma

www.digma.info 9. Jahrgang, Heft 4, Dezember 2009

Schwerpunkt:

Einwilligung

fokus: Einwilligung und ihre technische Umsetzung
report: Wunderheilmittel Videoüberwachung?
forum: Datenschutz ohne Grenzen



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

Schulthess §

inhalt

fokus

Schwerpunkt:
Einwilligung

Vertrauen muss man nicht lernen

Es ist viel von Vertrauen und Vertrauensverlust die Rede. Müssen wir (wieder) lernen zu vertrauen? Der stellvertretende Chefredaktor der Neuen Zürcher Zeitung meint nein, nicht vertrauen muss man lernen, sondern misstrauen. Das stimme hoffnungsvoll – stimmt!

Konsens über alles – koste es, was es wolle?

Soll ein Einzelner in souveräner Willkür bewirken können, dass relevante Forschung unterbleibt und gesellschaftlicher Schaden entsteht, obwohl auf seiner Seite kein nachvollziehbares Interesse entgegensteht? Der Kriminologe hinterfragt den Grundsatz der Einwilligungsforschung mit Beispielen aus der Sozialforschung.

Einwilligung und ihre technische Umsetzung

Obwohl das Prinzip der Einwilligung ein tragendes Element des heutigen Datenschutzes ist, wurde nur wenig Fortschritt in seiner technischen Umsetzung gemacht. Die adäquate Behandlung der Einwilligung stellt eine gravierende praktische Herausforderung dar. Wie können Individuen in die Lage versetzt werden, ihre Einwilligung zum Gebrauch ihrer persönlichen Daten unmissverständlich auszudrücken und diese, wenn gewünscht, auch wieder zurückzuziehen? Auf der anderen Seite müssen Datenverarbeiter in der Lage sein festzustellen, ob für gewisse Informationen der Besitzer eingewilligt hat oder ob dafür eine Einwilligung benötigt wird.

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 99.00 (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

Wunderheilmittel Videoüberwachung?

Videoüberwachung boomt. Zwar wird eine gesetzliche Grundlage verlangt – doch bloss formale Regelungen reichen nicht aus. Der Zweck muss im Mittelpunkt stehen, damit vorher die Verhältnismässigkeit beurteilt und hinterher die Wirksamkeit evaluiert werden kann.

Private Überwachung im öffentlichen Raum

Private können sich gegen Videoüberwachung durch andere Private nur auf dem zivilrechtlichen Weg zur Wehr setzen. Die Statuierung einer Bewilligungspflicht für gesteigerten Gemeingebrauch würde es den Behörden ermöglichen, Überwachungen, welche nicht mehr bestimmungsgemäss und gemeinverträglich sind, kontrolliert zuzulassen.

Datenschutz ohne Grenzen

Der Safe-Harbor-Beitrag in digma 2009.3 lädt zu einer vertieften Auseinandersetzung mit dem Thema der grenzüberschreitenden Datenbekanntgabe ein. Der Beitrag legt die wichtigsten Punkte dar, die bei der Überprüfung der Rechtmässigkeit einer solchen Datenbekanntgabe zu beachten sind.

report

forum

ISSS

ICT Risk Management – noch zeitgemäss?

Liliane Mollet, Master of Law, CAS Information Security, Ergonomics AG, ISSS Vorstand liliane.mollet@isss.ch

Daniel Graf, Informatikstrategieorgan Bund, IS-Beauftragter Bund, ISSS Vorstand daniel.graf@isb.admin.ch

Wie ein Blick in die berühmte Kristallkugel scheint heute das Voraussehen von Ereignissen und deren Auswirkungen. Die aktuelle Wirtschaftslage zeigt dies nur allzu deutlich: Der Umgang mit Bedrohungen und Risiken stellt uns alle vor grosse Herausforderungen. Auch die Informationstechnologie muss Risiken erfassen, beurteilen und behandeln. Fehler, Ausfälle, Datenverluste oder menschliches Fehlverhalten im Umgang mit Informationstechnologie fordern Unternehmen wie Verwaltung zunehmend. ICT Risk Management ist ein wichtiger Bestandteil des Gesamtrisikomanagements einer Organisation. Doch wie viel Aufwand für ein ICT Risk Management ist sinnvoll? Worin liegt der Nutzen? Ist der klassische Ansatz der Beurteilung von Risiken noch der Richtige (Eintretenswahrscheinlichkeit x Schadensausmass = Risiko)?

Mit diesen und anderen Fragen beschäftigte sich die 12. Berner Tagung für Informationssicherheit, organisiert vom Verein Information Security Society Switzerland (ISSS) sowie dem Informatikstrategieorgan Bund (ISB) und moderiert durch Stephan Klapproth.

Sind Risiken berechenbar?

Eröffnet wurde die Tagung von Peter Fischer (Delegierter des ISB). Keynote-Referent Dr. Rudolf Baer, (BSG Unternehmensberatung St. Gallen) zeigte mit fundierten Argumenten auf (u.a. am Beispiel des schwarzen Schwans), wie unbrauchbar die allerorts empfohlene und angewandte Art ist (auch der ISO-Standards), Risiken zu berechnen und einzuschätzen. Versicherungen, beispielsweise, können Risiken nur aufgrund von langjährigen Beobachtungen, sorgfältigen Aufzeichnungen, gesetzmässiger Beschreibbarkeit von Ereignissen sowie sehr vielen stattgefundenen Ereignissen (z.B. Hausbrände) berechnen und beurteilen. Für den einzelnen Versicherten ist dies nicht möglich. Es gibt kein Gesetz der grossen Zahl für den Einzelfall. Weder den Autounfall noch den Brand eines Rechenzentrums oder das Eindringen eines Hackers kann man vorausberechnen. Die Eintrittswahrscheinlichkeit *eines* zukünftigen Ereignisses lässt sich nicht vorhersagen. Auch das Schadensausmass beim Eintreten eines bestimmten Ereignisses ist nicht einfach so zu berechnen. In einem Spital zum Beispiel kann der kleine Tippfehler am PC die Bedrohung eines Menschenlebens im OP bedeuten. Die Komplexität von Ursache und Wirkung entzieht sich jeglicher Wahrscheinlichkeitsrechnung. Baer zeigt schliesslich auf, wie man es besser machen könnte. Die Business-Prozesse den schlimmsten Bedrohungen eines Unternehmens gegenüber stellen (und nicht den Risiken). «Tun Sie das Zumutbare, um das Voraussehbare abzuwenden.»

Wie wichtig die korrekte Führung durchs Management ist, zeigte Dr. Urs E. Zurfluh (Verwaltungsrat CSS Versicherung) im nächsten Referat. Risk Management sei in der IT ein einfaches, praktikables und wirksames Führungsinstrument. Risiken müssten zudem fair bewertet und auf einen akzeptablen Wert reduziert werden. Mittel müssten gezielt eingesetzt werden. Schliesslich sei Kultur und Kommunikation sehr wichtig – also wie man als Unternehmen gegen Aussen mit Risiken umgeht.

Skeptisch gab sich Frank Thonüs (Country Manager, Symantec Switzerland) gegenüber den Äusserungen der Unternehmens-Riskmanager sowie dem Verhalten der PC-User. Anschaulich vermittelte er einen Überblick über die heutigen Bedrohungen und Risiken (z.B. wurden im Jahre 2008 um die 285 Mio. Datensätze gestohlen oder 75 000 aktive Bot-infizierte Computer pro Tag gezählt). Um die Kontrolle über die eigene IKT und die Daten wieder zu erlangen, fasste Thonüs die Thematik in vier Punkten zusammen:

- Infrastruktur schützen (Endpoint Protection);
- IKT-Richtlinien entwickeln und umsetzen (Control & Compliance);
- Informationen schützen (Data Loss Prevention);
- Systeme verwalten (Endpoint Management).

Sicherheitsprodukte seien das eine. Doch schliesslich brauche es im Unternehmen

eine Strategie. Hierfür braucht es Menschen, die das Risk Management beherrschen, und Menschen, die dieses umsetzen.

Social Media: Risiko und Chance

Wie es um die Risiken beim «Twittern», «Chatten» und «Googeln» steht, erläuterte im zweiten Teil der Veranstaltung Andreas Wuchner (IT Risk Space) anhand eindrücklicher Zahlen und vorgefallenen Ereignissen. Bei 200 Millionen registrierten Usern auf myspace.com oder bei monatlich 31 Milliarden Suchanfragen auf Google ist schon eine gewisse Vorsicht im Netz geboten. Die Kommunikation hat sich mit dem Aufkommen von Social Media grundlegend geändert. Gerade jetzt (während der Tagung) oder gar in der Nacht, während man schlafe, können Menschen im Internet über einen oder sein Business reden und man wüsste wohl nicht einmal davon. Einer könnte gezielt über eine Firma im Netz Unwahrheiten verbreiten und damit deren Image gefährden. Deshalb sei es wichtig zu überlegen, was es für Möglichkeiten gäbe. Social Media sollte als Chance (und nicht nur als Verhinderung) gesehen werden. Die Diskussionen über die eigene Firma, zum Beispiel in einem Blog, könne man selbst steuern (Risiko minimieren). Fazit: Verstehen, was die Kinder zu Hause machen (chatten, twittern, …) – dann versteht man auch, welche Möglichkeiten die sozialen Netzwerke einem selbst und seinem Unternehmen bieten können und wie man damit umgehen soll.

Rechtliche Verantwortung

Wie es mit der rechtlichen Verantwortung fürs ICT Risk Management aussieht, zeigte Dr. Wolfgang Straub (Anwaltskanzlei Deutsch Wyss & Partner) auf. Schäden durch ungenügende Informationssicherheit können zu Verantwortlichkeitsansprüchen gegenüber Verwaltungsräten und Geschäftsleitungsmitgliedern führen. Zudem können Mitarbeitende aller Stufen für Versäumnisse aus Arbeitsrecht zur Verantwortung gezogen werden. Solche Haftungsansprüche setzen jedoch eine Verletzung von Sorgfaltspflichten voraus. Im Bereich der Informationssicherheit ist von entscheidender Bedeutung, ob ein angemessenes und nachvollziehbares Risk Management erfolgte (Dokumentieren der eigenen Sorgfalt). Obschon es bisher in der Schweiz kaum Gerichtsentscheide zu mangelnder Sorgfalt beim Umgang mit IT-Risiken gibt, nehmen die Verantwortlichkeitsklagen generell zu. Jedoch könnte der Gang vor den Richter auch kontraproduktiv sein. Manchmal kann es für Unternehmen besser sein (Reputation), wenn sie zusammen mit der Marketingabteilung eine gute Antwort zu einem Vorfall verfassen. Wichtig sind ausserdem gut formulierte Verträge (Planung, Steuerung, Risikoübertragung regeln).

Teamwork bei Tempo 1000

Eindrücklich und nachvollziehbar zeigte Daniel Siegenthaler (Pilot Patrouille Suisse), wie Risk Management sowohl in der Luft als auch am Boden umgesetzt wird. Patrouille Suisse steht für Präzision, Zuverlässigkeit und Sicherheit. Dies ist nur dank einem klar definierten Ziel und dem gemeinsamen Vorgehen möglich. Zudem erreicht ein effizientes Team mehr, als gleich viele Einzelpersonen jemals erreichen könnten. Ehrliche und offene Kommunikation, hundertprozentiges Vertrauen und entsprechende Teamführung minimieren die Risikofaktoren und machen sie für die Piloten zu einer kalkulierbaren Grösse.

Fazit

Solides ICT Risk Management ist nur mit einer klaren Strategie und offener Kommunikation möglich. Weniger die Formel, die Berechnung, sondern mehr die Führung eines Unternehmens, die Art der Kommunikation und Zusammenarbeit ist von Bedeutung. Ob dies die künftige Lösung für ein nachhaltiges ICT Risk Management ist und der klassische Ansatz bald auch in den Standards abgelöst wird, bleibt weiterhin offen. ■

Literatur, weiterführende Links

Die Referate der 12. Berner Tagung und weitere Veranstaltungen der Information Security Society Switzerland finden Sie unter <http://www.isss.ch/>.

Kurz&bündig

An der 12. Berner Tagung für Informationssicherheit vom 26. November 2009 setzten sich die Referenten mit der Frage nach Aufwand und Nutzen eines ICT Risk Managements auseinander. Ob der klassische Ansatz der Risikoanalyse (R=ExA) weiterhin angewendet werden kann oder ob man vielmehr den «schwarzen Schwan» berücksichtigen muss, wird die nicht vorhersehbare Zukunft weisen. Die Risiken sind vielfältig und komplex. Aber durch ein bewusstes Angehen eines ICT Risk Managements mit klaren Strategien und offener Kommunikation lassen sich Bedrohungen erkennen und die Auswirkungen beim Eintreten eines (unerwünschten) Ereignisses reduzieren und kontrollieren.

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 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
Homepage: www.schulthess.com

Schulthess §