Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info

12. Jahrgang, Heft 3, Oktober 2012

Schwerpunkt:

Online-Marketing

fokus: Herausforderung Online-Marketing

fokus: Eine Balance zwischen Nutzen und Schutz

report: Google Street View: On the road again?

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

Schulthess §

fokus

Schwerpunkt:
Online-Marketing

auftakt
Compliance-Fragen auch beim Staat
von Isaac Reber Seite 93

Online-Marketing auf dem Prüfstand
von Bernhard M. Hämmerli Seite 96

Herausforderung Online-Marketing
von Tobias Kollmann/
Julia Tanasic Seite 98

Online-Marketing – Trends und Prognosen
von Leonardo Kopp Seite 104

Online-Marketing und Datenschutz
von Rolf H. Weber Seite 110

Eine Balance zwischen Nutzen und Schutz
von Marc Langheinrich/
Günter Karjoth Seite 116

Herausforderung Online-Marketing

Mit dem Online-Marketing werden eigene Mechanismen für die Absatzpolitik in der Net Economy entwickelt. Angepasste und neue Marketinginstrumente zielen im Online-Marketing auf die Ermöglichung einer Integration des Kunden und auf eine verbesserte Kundenansprache durch Personalisierung und Individualisierung.

Online-Marketing und Datenschutz

Die Zahl von Online-Marketing-Vorkehren steigt rasant an. Dadurch erhöhen sich die Risiken für die Einhaltung der Datenschutzprinzipien. Der Gesetzgeber dürfte oft zu spät sein. Können neue rechtliche Rezepte – zum Beispiel die Fruchtbarmachung des UWG – helfen?

Eine Balance zwischen Nutzen und Schutz

Aus Sicht der Webseiten-Besitzer ist Web Tracking wünschenswert. Aus Sicht der Benutzer sind grössere Benutzerprofile problematisch, da sie Beziehungen enthalten können, die nicht an Unbekannte gelangen sollten. Wie funktioniert Web Tracking, welche Daten können gesammelt werden und welche Möglichkeit gibt es, sich dem zu entziehen?

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

Rubrikenredaktorin: Dr. iur. Sandra Husi-Stämpfli

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

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

Informations-sicherheit in der Gesetzgebung

Informationssicherheitserlasse und Selbstregulierungsstandards helfen, die aufgrund der voranschreitenden Informatikdurchdringung von Verwaltungs- und Geschäftsprozessen bestehenden Risiken zu minimieren. Was sollten die Erlasse regeln?

Google Street View: On the road again?

Das Bundesgericht hat sein Urteil über Google Street View gefällt. Der Beitrag stellt die Entscheidung dar, die dem EDÖB in fast allen Punkten Recht gibt und von den Medien trotzdem als Sieg von Google beschrieben wurde. Ausserdem wird auf kritische Punkte hingewiesen.

Aus den Daten-schutzbehörden

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

Online-Marketing

Warum nervt Online-Marketing eigentlich so? Unser Cartoonist erklärt es Ihnen.

report

Rechtsetzung
Informationssicherheit in der Gesetzgebung
von Barbara Widmer Seite 124

Forschung
Bürgersicht auf Sicherheit und Privatheit
von Michael Friedewald/ Johann Čas Seite 130

Rechtsprechung
Google Street View: On the road again?
von Amédéo Wermelinger Seite 134

forum

privatim
Aus den Datenschutzbehörden
von Sandra Husi-Stämpfli Seite 140

ISSS
Bring your own device: Chancen und Risiken
von Daniel Graf Seite 142

agenda Seite 143

schlusstakt
Ansichten über Strassen und Hecken
von Bruno Baeriswyl Seite 144

cartoon
von Reto Fontana

Rechtsetzung

Informationssicherheit in der Gesetzgebung[1]

Barbara Widmer, lic. iur., LL.M., CIA, Juristin beim Datenschutzbeauftragten des Kantons Basel-Stadt, Basel barbara.widmer@dsb.bs.ch

«Risiken gilt es zu minimieren. Ist dies nicht möglich, muss man sie wenigstens kalkulieren» (Marc Ruef, 2004)[2].

Die rasant voranschreitende Durchdringung der Geschäfts- und Verwaltungsprozesse mit Informationstechnik bringt einerseits massgebliche Vorteile, birgt andererseits aber auch erhebliche Risiken. Treten diese ein, können sie unerwünschte Auswirkungen auf die Geschäftstätigkeit bzw. die Aufgabenerfüllung sowie die Reputation haben und je nach Sachlage auch Haftungsansprüche Dritter auslösen[3]. Entsprechend gilt es diese IT-spezifischen Risiken, gleich wie andere Risiken, mittels eines effektiven Risikomanagements zu bewirtschaften[4]. Dabei liegt die Verantwortung für die Sicherstellung der Einführung und Überwachung eines solchen auf der obersten Führungsebene[5] (im Staatswesen beim Bundes-, Regierungs- oder Gemeinderat und in Unternehmungen je nach Organisationsform beim Verwaltungsrat, Vorstand usw.)[6].

Risikomanagement

Ein effektives Management von Risiken lässt sich nur dann erreichen, wenn eine klar definierte IT-Governance sowie eine sich an dieser orientierende IT-Sicherheitsstrategie vorhanden sind. Eine klar definierte IT-Governance umfasst dabei neben der Steuerung und Kontrolle von Risiken auch die Spezifizierung von Verantwortlichkeiten und Entscheidungsbefugnissen innerhalb der Informationstechnik, deren strategische Ausrichtung, die Sicherstellung von Mehrwertschaffung sowie die zielgerichtete Verteilung und Zuweisung von Ressourcen[7]. Die IT-Sicherheitsstrategie legt ausgehend von der für massgeblich erklärten IT-Governance die grundlegenden Sicherheitsprinzipien und Sicherheitsziele des Staatswesens oder der Unternehmung fest. Sie statuiert die diesbezüglichen Vorgaben und stellt damit die Legitimationsgrundlage für alle Sicherheitsaktivitäten im jeweiligen Staatswesen oder der jeweiligen Unternehmung dar[8]. Im Weiteren nimmt sie im Zusammenhang mit der Informationssicherheit eine Zuweisung der zentralen Funktionen und Zuständigkeiten vor. Entsprechend diesen Inhalten liegt auch die Verantwortung für die Erstellung und Überwachung der IT-Governance und der IT-Sicherheitsstrategie auf der obersten Führungsebene eines Staatswesens oder einer Unternehmung[9].

Sowohl IT-Governance als auch Informationssicherheit stellen globale Themenbereiche dar. Der Grund dafür liegt darin, dass sich alle privaten und staatlichen Einheiten, die Informatikanwendungen betreiben, unabhängig von ihrer gesetzlichen Grundlage, ihrem Geschäfts- und Verwaltungsbereich sowie ihrer örtlichen Ansiedlung mit diesen auseinandersetzen müssen (wenn auch in unterschiedlicher Ausgestaltung und Intensität). Entsprechend hat sich auch die inhaltliche Ausgestaltung der IT-Governance und Informationssicherheit global entwickelt. Dies lässt sich insbesondere daran erkennen, dass deren Inhalte in erheblichem Umfang in international anerkannten Rahmenwerken (Selbstregulierungs-Standards) festgelegt sind. Die bekanntesten dieser Rahmenwerke[10] sind Cobit[11], ISO 2700X[12] und BSI[13].

Informationssicherheitserlasse und ihre Inhalte

Regelungsformen

Ausgehend von den Inhalten der vorgenannten internationalen Rahmenwerke sowie allfälliger bereichsspezifischer gesetzlicher Vorgaben[14] haben Privatunternehmen ihre Informationssicherheitsleitlinien und das Staatswesen seine Informationssicherheitserlasse geschaffen. Die Informationssicherheitserlasse des Staats-

wesens finden sich dabei verbreitet in Form von Verordnungen. So im Bund z.B. in der Bundesinformatikverordnung[15] oder in den Kantonen in kantonalen Informationssicherheitsverordnungen[16]. Inhaltlich weisen diese Erlasse sehr unterschiedliche Strukturen auf und erscheinen in ihrem Aufbau nicht immer konsistent. Verallgemeinernd kann jedoch festgehalten werden, dass entsprechende Erlasse neben den allgemeinen einleitenden (Zweck, Gegenstand, Geltungsbereich usw.) und abschliessenden (Übergangs- und Schlussbestimmungen) Regelungen *mindestens* folgende Themenbereiche behandeln sollten: Definition der verwendeten Begriffe, strategische und organisatorische Grundlagen und Voraussetzungen sowie die Zuständigkeiten und Verantwortlichkeiten in der Umsetzung[17]. Gestützt auf diese Ausgangslage soll die inhaltliche Ausgestaltung dieser Themenbereiche nachfolgend eingehender beleuchtet werden.

Begriffsdefinitionen

Da unter ein und demselben Begriff oft ein Mehrfaches verstanden werden kann, ist es unerlässlich, die im Rahmen eines entsprechenden Erlasses verwendeten (Fach-)Begriffe zu definieren. Dies gilt insbesondere für den Begriff der Informationssicherheit selbst. Wie sich dieser genau definiert, lässt sich der massgeblichen Literatur nicht schlüssig entnehmen. Teilweise wird derselbe gleichbedeutend mit IT-Sicherheit verwendet und teilweise wird davon ausgegangen, dass der Begriff «Informationssicherheit» sowohl Informationen in Papierform als auch elektronisch bearbeitete Informationen umfasst, während sich der Begriff «IT-Sicherheit» lediglich auf elektronisch bearbeitete Informationen bezieht[18]. Da es sich bei der Informationssicherheit somit nicht um einen allgemein festgelegten Begriff handelt, ist es unerlässlich, diesen für den jeweiligen Anwendungsbereich einheitlich zu definieren.

Strategische und organisatorische Inhalte

Hinsichtlich der strategischen Inhalte kann es sich für das Gesamtverständnis lohnen, Bezug auf die für eine effektive und effiziente Informationssicherheit notwendigen Grundlagen zu nehmen. Im Sinn eines Einleitungsparagraphen lässt sich z.B. festhalten, dass Grundlage für eine effektive und effiziente Informationssicherheit eine festgelegte IT-Governance und Informatikstrategie, ein daraus abgeleitetes Risikomanagement, eine der Umsetzung des Risikomanagements dienende IT-Sicherheitsstrategie sowie die Sicherstellung der Umsetzung der IT-Sicherheitsstrategie (inkl. zeitgerechte Anpassung derselben an veränderte Verhältnisse) bilden.

Im Rahmen der organisatorischen Inhalte empfiehlt sich eine Aufnahme von Regelungen zu den Rollen, die es im Umfeld der Informationssicherheit zu besetzen gilt sowie zu den mit diesen verbundenen Aufgaben. Die zwei wichtigsten Funktionen in diesem Zusammenhang sind ein Organ, das sich mit strategischen Fragestellungen befasst (Strategieorgan) und einen Informationssicherheitsbeauftragten, der die Sicherheitsbelange koordiniert und innerhalb des Staatswesens vorantreibt. Dem mit der Strategie befassten Organ sollten dabei mindestens die folgenden Aufgaben übertragen werden:

- die Sicherstellung der Ausarbeitung einer IT-Sicherheitsstrategie unter Einbezug der im Rahmen des Risikomanagements identifizierten Risiken;
- die Festlegung von generellen Sicherheitsmassnahmen zur effektiven und effizienten Umsetzung der ausgearbeiteten IT-Sicherheitsstrategie;
- die Sicherstellung der Umsetzung der festgelegten IT-Sicherheitsstrategie sowie deren zeitgerechte Anpassung an veränderte Verhältnisse[19] sowie
- die regelmässige Information der obersten Führungsebene über die eigene Arbeit und den Stand der Informationssicherheit im jeweiligen Staatswesen[20].

Das Strategieorgan ist auch mit Personen zu besetzen, die über fundierte Infor-

Kurz&bündig

Informationssicherheitserlasse sollten neben den allgemeinen einleitenden (Zweck, Gegenstand, Geltungsbereich usw.) und abschliessenden (Übergangs- und Schlussbestimmungen) Regelungen *mindestens* folgende Themenbereiche behandeln: Definition der verwendeten Begriffe, strategische und organisatorische Grundlagen und Voraussetzungen sowie die Zuständigkeiten und Verantwortlichkeiten in der Umsetzung. Allerdings können entsprechende Erlasse ihre Funktionen nur dann wahrnehmen, wenn die sich daraus ergebenden Verantwortlichkeiten von den Betroffenen anerkannt werden und die jeweils Verantwortlichen aktiv mitdenken und sich nicht auf die Verwaltung des bereits Vorhandenen beschränken.

mationssicherheitskenntnisse verfügen[21]. Ergänzend sollte diesem aber die Kompetenz eingeräumt werden, zur Erfüllung seiner Aufgaben interne und/oder externe Fachpersonen beizuziehen und insbesondere auch spezialisierte Fachkommissionen einzusetzen[22]. Dessen organisatorische Ausgestaltung kann in einem Organisationsreglement festgelegt werden.

Im Weiteren gilt es einen Informationssicherheitsbeauftragten einzusetzen. Abhängig von der Grösse und der Organisation des Staatswesens kann es sich dabei um eine Einzelperson oder ein Team handeln[23]. Der Informationssicherheitsbeauftragte ist für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Staatswesens zuständig und sollte mittels entsprechender Regelung mindestens mit folgenden Aufgaben betraut werden:

- mit der Unterstützung des für die Strategie verantwortlichen Organs bei der Wahrnehmung seiner Aufgaben;
- der Unterstützung der Leistungsbezüger (siehe unten) bei der Umsetzung der sich aus der IT-Sicherheitsstrategie ergebenen organisatorischen und technischen Massnahmen sowie
- der inhaltlichen Vermittlung zwischen Leistungsbezügern und Leistungserbringern (siehe unten)[24].

In der Regel empfiehlt sich eine zentrale Einsetzung des Informationssicherheitsbeauftragten[25] (allenfalls ergänzt durch für Informationssicherheit zuständige Personen bei den Leistungsbezügern). In hierarchischer Hinsicht sollte dieser mindestens auf Stabsebene[26] und im Verhältnis zwischen den Leistungsbezügern und Leistungserbringern neutral[27] angesiedelt sein.

Umsetzungszuständigkeit und -verantwortlichkeit

Die Zuständigkeit für die Umsetzung der vom Strategieorgan beschlossenen Vorgaben liegt einerseits bei den von diesem eingesetzten Fachkommissionen sowie den Leistungsbezügern und den Leistungserbringern. Die Fachkommissionen unterstützen das Strategieorgan dabei im Hinblick auf die taktische und operative Umsetzung und arbeiten zu seinen Händen Entscheidungsgrundlagen aus. Die Leistungsbezüger und Leistungserbringer sind anschliessend für die Umsetzung der vom Strategieorgan beschlossenen und den Fachkommissionen konkretisierten Vorgaben verantwortlich. Die Leistungsbezüger bezeichnen dabei die verschiedenen Verwaltungseinheiten eines Staatswesens, die Informatikdienstleistungen beziehen, und die Leistungserbringer verwaltungsinterne oder -externe Informatikdienstleister. Entsprechend sollten diese beiden Begriffe (im Sinn von Rollen im Umsetzungsbereich der Informationssicherheit) in einem Informationssicherheitserlass eingeführt sowie auch definiert werden.

Die Leistungsbezüger sind in ihrem Zuständigkeitsbereich dafür verantwortlich, dass die sich aus den Vorgaben des Strategieorgans ergebenden Sicherheitsmassnahmen umgesetzt und zeitgerecht an veränderte Verhältnisse angepasst werden. Ihnen sollten mittels entsprechenden Regelungen insbesondere folgende Aufgaben zugeteilt werden:

- Führung eines Verzeichnisses der vorhandenen Informationsbestände und Informatikanwendungen;
- Ermittlung des Schutzbedarfs der vorhandenen Informationsbestände und Informatikanwendungen[28];
- Erstellung eines dem oben genannten und ermittelten Schutzbedarf entsprechenden Massnahmeplans[29]. Dieser

Literatur

- Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 2.0 (zu finden unter <http://www.bsi.bund.de/gshb>) (zit. BSI-Standard 100-2).
- Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, Basis für Informationssicherheit 2011 (zu finden unter <http://www.bsi.bund.de/grundschutz>) (zit. IT-Grundschutz-Kataloge).
- IT Governance Institute/KPMG, IT Governance für Geschäftsführer und Vorstände, 2. Aufl. 2003 (zu finden unter <http://www.isaca.org/German/Documents/Board-Briefing-on-IT-Governance-German.pdf>) (zit. IT-Governance-Leitfaden).
- Thomas Schlienger, Informationssicherheitskultur in Theorie und Praxis, Diss. Freiburg i.Ü. 2006.
- Jürg Schneider, Informationssicherheit in der IT und persönliche Haftung der Verwaltungsräte, Basel 2008.
- Rolf H. Weber, Risikomanagement durch Einhaltung von IT-Sicherheitsstandards in: sic! 3/2004, 181 ff.
- Rolf H. Weber/Annette Willi, IT-Sicherheit und Recht, Grundlagen eines integrativen Gestaltungskonzepts, Zürich/Basel/Genf 2006.
- Bruno Wildhaber, Informationssicherheit, Rechtliche Grundlagen und Anforderungen an die Praxis, Diss. Zürich 1993.
- Annette Willi, IT-Governance als Aufgabe des Verwaltungsrates, Diss. Zürich 2008.
- Bernhard Witt, IT-Sicherheit kompakt und verständlich, Eine praxisorientierte Einführung, Wiesbaden 2006.

sollte dabei regelmässig auf seine Zweckmässigkeit und Aktualität überprüft werden und mindestens Regelungen zu den folgenden Punkten enthalten: zur Erstellung und Verwaltung eines Zugriffs- und Berechtigungskonzepts, zur Datenaufbewahrung und Löschung unter Einhaltung allfälliger Aufbewahrungs- und Archivierungsvorschriften, zum Informationsaustausch mit Dritten sowie zum Einbezug der Mitarbeitenden in den Sicherheitsprozess.

Die Leistungserbringer sind dagegen für die Entwicklung und/oder Bereitstellung und/oder den Unterhalt der Informatikanwendungen und technischen Mittel verantwortlich, welche die Leistungsbezüger unter Einhaltung der informationssicherheits- und datenschutzrechtlichen Vorgaben zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Damit sie diese Aufgabe wahrnehmen können, müssen die Leistungsbezüger sie über die gesetzlichen Anforderungen hinsichtlich Datenschutz und Informationssicherheit informieren.

Da das Verhältnis zwischen Leistungsbezügern und Leistungserbringern nicht ohne Risiko ist (Abgrenzung von Verantwortlichkeiten, Leistungsstörungen usw.), sollte der Informationssicherheitserlass eine Regelung enthalten, wonach die gegenseitigen Rechte und Pflichten sowie die Anforderungen an die Bereitstellung und Nutzung der vereinbarten Informatikdienstleistungen in Dienstleistungsvereinbarungen (Service Level Agreements, SLA) schriftlich zu regeln sind. Entsprechende Dienstleistungsvereinbarungen können dabei entweder als Anhang zu einer Rahmenvereinbarung oder als eigenständige Verträge ausgearbeitet sein.

Schlussfolgerungen

Informationssicherheitserlasse und Selbstregulierungs-Standards helfen einerseits, die aufgrund der stets voranschreitenden Informatikdurchdringung von Verwaltungs- und Geschäftsprozessen bestehenden Risiken zu minimieren und, wo dies nicht möglich ist, zu kalkulieren. Diesen kommt somit eine wichtige und für jedes Staatswesen und jede Unternehmung unverzichtbare Rolle zu. Allerdings ist in deren Zusammenhang Folgendes zu beachten: Entsprechende Regelwerke können ihre Funktionen nur dann wahrnehmen, wenn die sich daraus ergebenden Verantwortlichkeiten von den

Fussnoten

1 Der vorliegende Artikel basiert auf Erfahrungen aus Gesetzgebungsarbeiten im Zusammenhang mit einer neuen Informationssicherheitsverordnung für den Kanton Basel-Stadt. Er ist das Resultat einer intensiven Auseinandersetzung mit den sich im Rahmen von Informationssicherheit stellenden rechtlichen, organisatorischen sowie informationstechnischen Fragen. Mein spezieller Dank gebührt in diesem Zusammenhang lic. rer. pol. Georges Hatt, Informationssicherheitsbeauftragter des Kantons Basel-Stadt (bis Ende März 2012) sowie Markus Brönnimann, Informatiker NDS FH, CAS IT-Security, Informatikrevisor beim Datenschutzbeauftragten des Kantons Basel-Stadt. Die beiden sind mir bei der Ausarbeitung der entsprechenden Verordnungsvorlage mit ihrer jahrelangen Erfahrung im IT- und Informationssicherheits-Bereich stets fachkundig und engagiert zur Seite gestanden. Die Verordnungsvorlage sowie die dazu verfassten Erläuterungen werden voraussichtlich im Herbst/Winter 2012 in die kantonale Vernehmlassung gehen.

2 Siehe zur Person von Marc Ruef <http://www.computec.ch/mruef> (besucht am 6.8.2012).

3 Wildhaber, 43 f.

4 Siehe für das IT-Risikomanagement Witt, 99 ff.

5 Weber/Willi, 197 ff; BSI-Standard 100-2, Ziff. 3.1.

6 Siehe für diesen Abschnitt auch IT-Grundschutz-Kataloge, Ziff. 1.1.

7 IT-Governance-Leitfaden, 13; siehe dazu auch Willi, 16 ff.

8 Schneider, 48; Weber/Willi, 188 f.

9 IT-Governance-Leitfaden, 12 f; Weber/Willi, 189 f; siehe dazu auch Weber in: sic!, 3/2004, 182 f.

10 Siehe dazu auch Schlienger, 47 ff; Weber/Willi, 68 ff. Siehe für die Bedeutung und Funktion dieser Rahmenwerke Weber in: sic! 3/2004, 185 ff.

11 COBIT = Control Objectives for Information and Related Technology: international anerkanntes Rahmenwerk zur IT-Governance, das vom IT-Governance-Institut herausgegeben wird. Es enthält eine Anleitung zur unternehmens- oder verwaltungsinternen Ausgestaltung der Informationstechnologie (siehe <http://www.isaca.ch/cobit.html>, besucht am 6.8.2012).

12 ISO = International Organisation for Standardization: Organisation, die für verschiedene Bereiche internationale Normen erarbeitet. Bei ISO 2700X handelt es sich um entsprechende Normen im Bereich der Informationssicherheit. Diese haben die Festlegung von Anforderungen zur Einführung, Bewirtschaftung, Dokumentation und fortlaufenden Verbesserung einer risikobasierten Informationssicherheit zum Ziel (siehe <http://www.iso.org>, besucht am 6.8.2012).

13 BSI = deutsches Bundesamt für Sicherheit in der Informationstechnik: Rahmenwerk, das Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Massnahmen im Zusammenhang mit Informationssicherheit enthält (siehe <http://www.bsi.bund.de>, besucht am 6.8.2012).

14 Z.B. bereichsspezifische Geheimhaltungs-, Aufbewahrungs-, Nachweis-, Sorgfalts- oder Gewährleistungspflichten.

Fussnoten (Forts.)

15 Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV), SR 172.010.58. Der Bundesrat hat das VBS beauftragt, bis Ende 2012 für den Bund ein neues Spezialgesetz über die Informationssicherheit zu erarbeiten. Er begründet diesen Schritt damit, dass die Bedrohungen im Bereich der Informationssicherheit in jüngerer Zeit stark zugenommen haben, was ein vernetztes und integrales Vorgehen erfordere (Jusletter 5, Dezember 2011, <http://www.jusletter.ch>, besucht am 6.8.2012). Zudem hat der Bundesrat eine Cyber-Strategie (wie mit Risiken in der Informationstechnik umgegangen werden soll) gutgeheissen. Zu deren Umsetzung sollen bis ins Jahr 2017 insgesamt 59 zusätzliche Stellen in der Bundesverwaltung und der Armee geschaffen werden (siehe NZZ vom 31. August 2012, 11).

16 Siehe z.B. Kanton Basel-Stadt: Verordnung vom 9. April 2002 zur Informatiksicherheit (ISV), SG 153.320; Kanton Basel-Landschaft: Verordnung vom 11. März 2008 über die Informationssicherheit (VIS), SGS 162.51; Kanton Luzern: Verordnung vom 2. Februar 2010 über die Informatiksicherheit, SRL Nr. 26b; Kanton Zürich: Informatiksicherheitsverordnung vom 17. Dezember 1997, LS 70.8; Kanton St. Gallen: Verordnung vom 24. Februar 2004 über die Informatiksicherheit, SG 142.21.

17 Siehe dazu auch Schlienger, 28 ff.

18 Siehe dazu Weber/Willi, 6 ff.

19 Schneider, 48.

20 Siehe zu den Aufgaben IT-Governance-Leitfaden, 71 f.

21 IT-Governance-Leitfaden, 72 f; Schneider, 48 f.

22 IT-Governance-Leitfaden, 73.

23 BSI-Standard 100-2, Ziff. 3.4.4; Wildhaber, 147.

24 Siehe für die Aufgaben der Informationssicherheitsbeauftragten BSI-Standard 100-2, Ziff. 3.4.4; Wildhaber, 147 f.

25 Wildhaber, 149.

26 BSI-Standard 100-2, Ziff. 3.4.4.

27 Siehe dazu auch Wildhaber, 149.

28 Wildhaber, 145.

29 Wildhaber, 145 f.

30 In Anlehnung an ein Zitat von Norbert Blüm, promovierter Philosoph, Autor und Kabarettist sowie ehemaliger CDU-Politiker (Norbert Blüm war von 1982 bis 1998 Bundesminister für Arbeit und Sozialordnung in der Deutschen Regierung).

Betroffenen anerkannt werden. Dies ist mitunter im staatlichen Umfeld nicht immer der Fall und kann je nach Ausmass der nicht wahrgenommen Verantwortlichkeiten zu spürbaren Differenzen im Verhältnis von Soll und Ist führen. Im Weiteren verfügt das Leben insbesondere in einem sich so schnell entwickelnden und verändernden Umfeld wie der Informationstechnik und der mit dieser verbundenen Informationssicherheit regelmässig über mehr Fälle, als der Gesetzgeber sich vorstellen kann[30]. Eine effektive und effiziente Anwendung und Umsetzung von Informationssicherheit ist deshalb nur möglich, wenn die Verantwortlichen aller Hierarchiestufen aktiv mitdenken und sich nicht auf die Verwaltung der einmal erarbeiteten Grundsätze und Vorgaben beschränken. ■

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 §