Zeitschrift für Datenrecht und Informationssicherheit

digma

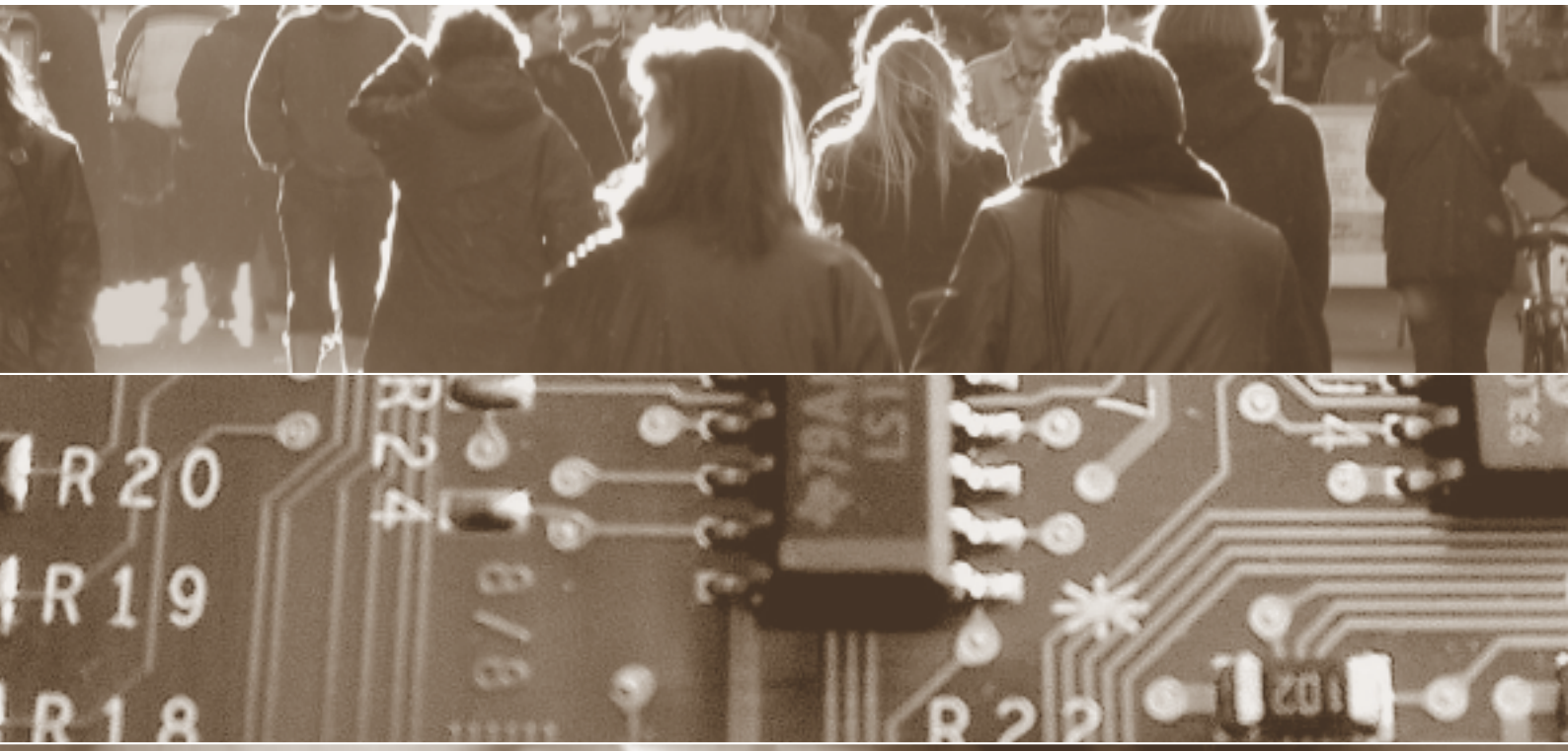
www.digma.info 8. Jahrgang, Heft 4, Dezember 2008

Schwerpunkt:

Cyber-Ermittlungen

fokus: Die Geschwätzigkeit des verlorenen Laptops
Cyber-Crime als Dienstleistung

report: Strategische Informationssicherheit



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

Schulthess §

fokus

Schwerpunkt:
Cyber-Ermittlungen

Die Geschwätzigkeit des verlorenen Laptops

Passwörter und Verschlüsselung sollen den unberechtigten Zugang zu Daten verhindern. Doch wie wirksam sind diese Massnahmen, wenn ein Computer abhanden kommt? Der Artikel zeigt, dass solche Laptops fast nichts für sich behalten können.

Cyber-Crime als Dienstleistung

Die Möglichkeiten im Internet haben nicht nur legitime Geschäftsfelder transformiert: Auch professionelle, gut organisierte Cyber-Verbrecher profitieren davon.

Incident Reponse Capabilities

IT-Sicherheit darf nicht mehr nur den Schutz der eigenen IT-Infrastruktur zum Ziel haben, sondern muss auch dazu beitragen, Schäden an Systemen von Dritten zu verhindern. Der Autor betont auch die Wichtigkeit, auf Sicherheitsvorfälle reagieren zu können, wenn die präventiven Schutzvorkehrungen nicht ausreichen.

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

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

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (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 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, zs.verlag@schulthess.com

Strategische Informations-sicherheit

Die Autorin hat in ihrer Dissertation Fallstudien zur Informationssicherheit in Grossunternehmen durchgeführt. Sie stellt fest, dass sich Informationssicherheit verschiebt von einem defensiv ausgerichteten hin zu einem Führungsinstrument, das einen Mehrwert für Unternehmen schafft.

ERP-Risiko-Management

In vielen Firmen werden wichtige Finanz- und Logistik-Prozesse, welche gesetzliche Compliance-Anforderungen erfüllen müssen, mit Hilfe von Enterprise-Resource-Planning-Managementsystemen abgedeckt. Eine ISSS-Tagung widmete sich verschiedenen Aspekten des Risikomanagements für ERP-Systeme.

Der «naked citizen» und sein Schwabbelbauch

Der Staatsschutz wird wieder aktiv, die Krankenkassen immer hungriger – aber der Bürger macht sich kaum Gedanken. Aber dann plötzlich … !

report

forum

ISSS

ERP-Risiko-Management

Dr. Alexander Herrigel, Senior Manager, SECUDE Global Consulting (Schweiz) AG, Regensdorf, ISSS Vorstand alexander.herrigel@isss.ch

Aufgrund der aktuellen Finanzkrise führte die Information Security Society Switzerland am 30. September 2008 eine Luzerner Fachtagung durch. Sie befasste sich mit den verschiedenen Aspekten des Risiko-Managements für Enterprise-Resource-Planning-Systeme (ERP-Systeme). Der Grund für den Fokus auf die ERP-Systeme bestand darin, dass in vielen Firmen wichtige Finanz- und Logistik-Prozesse, welche gesetzliche Compliance-Anforderungen erfüllen müssen, mit Hilfe von ERP-Systemen unterstützt werden.

Zentrale Fragestellungen

Da zahlreiche Vorfälle in angesehenen Weltkonzernen trotz der zunehmenden Regeldichte das Vertrauen der Öffentlichkeit in das Risikomanagement von Firmen oder Institutionen erschüttert und eine allgemeine Verunsicherung ausgelöst haben, war es die Zielsetzung der Tagung, Antworten zu den folgenden Fragen zu finden:

- Was sind die Management-anforderungen an das Risiko-Management?
- Welche gesetzlichen Anforderungen gibt es?
- Wie ist das Zusammenspiel zwischen Risiko-Kontrolle und Risiko-Management?

An der Tagung wurden zuerst in Fachvorträgen die verschiedenen Sichtweisen dargestellt. Danach wurden in parallelen Podiumsdiskussionen unter Einbezug von Fragen und Meinungen der Teilnehmenden wichtige Aspekte vertieft.

Verhindern oder Aufdecken?

Im ersten Vortrag legte Jürgen Müller, Systems & Process Assurance Leader Switzerland und Partner Pricewaterhouse-Coopers, dar, wie man eine gute Kontrolle von ERP-Daten- und Informationen erreicht, und präsentierte verschiedene Lösungsansätze:

- Restriktive Vergabe von Zugriffsrechten und Anwendung des 4-Augen-Prinzips gegen offene Zugriffsrechte
- Ausnutzen aller automatisierten Kontrollen im System versus flexiblem Set-Up von Geschäftsprozessen
- Integration des Workflows im Geschäftsprozess versus Workflow ausserhalb des Geschäftsprozesses
- kein SAP-ALL für alle Benutzer versus einige SAP_ALL Accounts

In seinem Vortrag zeigte Jürgen Müller, dass die Dimensionierung der Lösung von der Grösse, Komplexität und der Art des Geschäftes abhängt und empfahl, unbedingt einen Proof of Concept vor der eigentlichen Implementierung durchzuführen und die Meinung der Prozessverantwortlichen zwingend zu berücksichtigen.

Neue gesetzliche Anforderungen

Dr. iur. Fürsprech Beat Lehman stellte in seinem Vortrag die Neuerung im Gesellschafts- und Revisionsrecht vom 16. Dezember 2005 und die neuen Vorschriften zu den verschiedenen Formen der Revision und zur Risikokontrolle vor. Er beantwortete Fragen zur Risikobeurteilung im Anhang zur Jahresrechnung (Art. 663b Ziff. 12 OR). Es wurden die folgenden wichtigen Aspekte besprochen:

- Welche Gesellschaften unterstehen der Pflicht zur Durchführung einer Risikobeurteilung?
- Wer ist für die Durchführung der Risikobeurteilung verantwortlich?
- Kann der VR die Durchführung der Risikobeurteilung nach

Weiterführender Link

Weitere Veranstaltungen der Information Security Society Switzerland finden Sie unter http://www.isss.ch

Art. 663b Ziff. 12 OR delegieren?

- Welche Rollen spielen die Risiken aus dem Einsatz der Informatik bei der Risikobeurteilung nach Art. 663b Ziff. 13 OR?

Beat Lehmann betonte, dass nur die Existenz eines funktionierenden internen Kontrollsystems nachgewiesen werden muss. Das Ergebnis der Risikobeurteilung hingegen muss im Geschäftsbericht nicht offengelegt werden.

Compliance oder ROI

Oliver Hanke, Head of Strategic Control, Bank Julius Bär, zeigte in seinem Referat, in welchen Bereichen die Finanzdaten bei der Bank Julius Bär genutzt werden, und stellte die Anforderungen an eine ERP-Lösung aus Finanzsicht dar. Hierbei ging er ein auf Finanzbuchhaltung und Datensicherheit, Controlling und ERP sowie Strategic Controlling. Er leitete die folgenden qualitativen Anforderungen an ein ERP aus Finanzsicht ab:

- Zuverlässigkeit der Daten
- Ganzheitliches und striktes Autorisierungskonzept
- Abstimmbarkeit der Daten aus verschiedenen Quellen

Hierbei machte er deutlich, dass die Gewährleistung der genannten drei Punkte trotzdem auch folgende zwei Anforderungen erfüllen sollte: (1) Aufrechterhaltung der «Time-to-Market»-Verarbeitungsgeschwindigkeit und (2) Hoher Bedarf an einem industriespezifischen Customizing.

Operational Risk Framework der UBS

Thomas Kohler, zuständig für Information Risk Control bei der UBS, stellte in seinem Vortrag das Operational Risk Framework der UBS vor. Er zeigte, wie die UBS das Operational Risk Framework und das Operational Risk Inventory implementiert hat. Durch die Abgrenzungen zwischen Policies & Standards, Controlling, Reporting, Identification und Data Collection machte der Referent deutlich, welche wichtigen Komponenten das UBS Risk Framework besitzt und wie umfassend dieses in der Praxis eingesetzt wird. Er zeigte beispielsweise, wie in einem Selbstzertifizierungsprozess die Informationsbasis für eine operative Risiko-Beurteilung generiert wird, und demonstrierte an Hand des Mengengerüstes von über 8342 Kontrollstandards, mit 8200 involvierten Mitarbeitern und 107 683 zertifizierten Risiko-Punkten, wie eine SOX-Compliance in der Praxis professionell und umfassend erreicht werden kann. Für den Autor dieses Artikels war es unverständlich, wie bei einer so umfassenden Risikobeurteilung solche Mängel im Risikomanagement der Anlagestrategie auftreten können, die zu den hohen Verlusten und Wertberechtigungen führten.

Die Tagung wurde mit einem Apéro beendet, an dem alle Teilnehmenden persönliche Gespräche mit den Vortragenden und verschiedenen Podiumsleitern führen konnten. ■

Kurz&bündig

An der Luzerner Fachtagung vom 30. September 2008, organisiert von der Information Security Society Switzerland ISSS, wurden gesetzliche und organisatorische Aspekte des Risiko-Managements für ERP-Systeme behandelt. Unter anderem stellte die UBS ihr umfangreiches Operational Risk Framework vor und Beat Lehmann erklärte anschaulich die Folgen der neuen gesetzlichen Anforderungen an die revisionskonforme Risikokontrolle.

Nächste Nummer

Die nächste Ausgabe von digma erscheint im März 2009 und widmet sich schwerpunktmässig dem Thema **«Cloud Computing»**

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 §