Zeitschrift für Datenrecht und Informationssicherheit

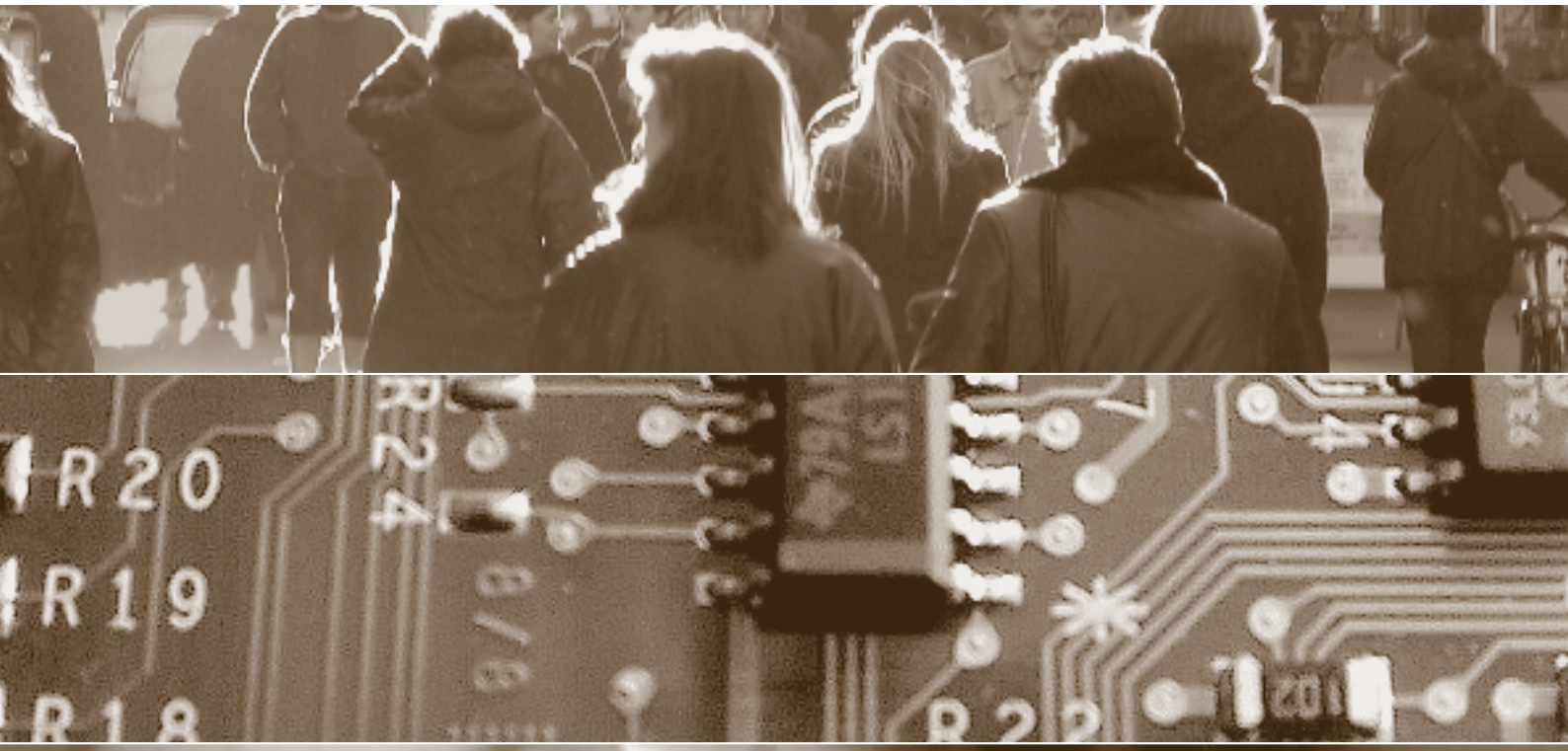
digma

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

Transfer

Das Risiko «Risk-Management»

Roland Portmann, Prof., Dozent für IT-Security, Hochschule Luzern – Technik & Architektur, externer Fachexperte bei ISO/IEC 27001-Zertifizierungen roland.portmann@hslu.ch

Eine vorbildliche KMU-Firma betreibt seit mehreren Jahren ein IT-Risk-Management. Die Risiken werden identifiziert, bewertet und in eine Risiko-Map eingetragen. Im Einverständnis mit der Geschäftsleitung werden Risiko-Minderungsmassnahmen getroffen, so dass sich die Farbe auf der Risiko-Map allmählich in Richtung grün bewegt. Der jährliche Zyklus führt dazu, dass nach vier bis fünf Jahren auf der Risiko-Map keine hohen und nur wenige mittlere Risiken ausgewiesen werden. Man fühlt sich sicher.

Dieses schulbuchmässige Vorgehen kann dazu führen, dass man sich in einer falschen Sicherheit wiegt.

Es muss ja besser werden!

In der Regel werden für hoch bewertete Risiken Minderungsmassnahmen getroffen. Da diese Massnahmen mit Kosten verbunden sind, erwartet die Geschäftsleitung, dass in den nachfolgenden Risiko-Analysen diese Risiken weniger kritisch bewertet werden. Die für die Durchführung der Risikoanalyse verantwortlichen Mitarbeiter sind damit einem unausgesprochenen Druck unterworfen, nach der Umsetzung der Risikominderungsmassnahmen die Bewertung in Richtung «Grün» zu ändern. Frühere Einschätzungen eines konkreten Risikos werden meistens nicht infrage gestellt, da man sich damit selber kritisieren würde.

In den nachfolgenden Ausführungen werden einige Probleme bei der Risikoanalyse im IT-Umfeld aufgezeigt.

Kennen Sie die IT-Risiken?

Bei einem Risikomanagement geht man davon aus, dass man alle wesentlichen Risiken kennt. Dies ist gerade in der Informationstechnologie aus den folgenden Gründen eine falsche Annahme:

- Die Technologie entwickelt sich rasant, so dass immer neue Risiken entstehen.
- Der Einsatz von Informationstechnologien nimmt in allen Bereichen immer noch rasant zu.
- Die Komplexität der IT-Infrastruktur erhöht sich kontinuierlich und nimmt bedrohliche Ausmasse an.
- Die Angriffe auf die IT-Infrastrukturen werden zunehmend hochprofessionell, so dass gängige Abwehrmassnahmen wie Malware-Protection zunehmend an Wirksamkeit verlieren.

Zwei Beispiele sollen die Problematik illustrieren:

- Das Risiko, dass gestohlene Daten ausländischen Behörden verkauft werden können, führte vermutlich vor einigen Jahren kaum ein Finanzinstitut auf der Risikoliste.
- Das Risiko, dass Malware entwickelt werden kann, die sich über Windowsrechner verbreitet, von keinem Virenscanner entdeckt wird und als einzige Schadfunktion die an Windows-Rechnern angeschlossene SPS-Steuerungen in einem genau definierten Umfeld gezielt manipuliert, hat man auch erst nach der Entdeckung von Stuxnet als Risiko identifiziert.

Es sind auch zunehmend Ereignisse denkbar, die bis heute noch nie eingetreten sind und daher nicht in einer Risiko-Analyse erscheinen:

- Die gesamte IT-Infrastruktur einer Firma könnte durch eine neuartige Malware schlagartig komplett lahmgelegt werden.
- Eine nicht detektierbare Malware könnte neben den heute üblichen Spionageaktivitäten auch interne Informationen verändern, um so die Geschäftstätigkeit zu schädigen.
- Eine Verseuchung der Smartphones aller Mitarbeiter mit einer Malware könnte zu einer Lahmlegung der Mail-Infrastruktur einer Firma führen.
- Das Internet könnte für längere Zeit ausfallen.

Diese Liste könnte beliebig erweitert werden. Wie geht man mit solchen Risiken im Risk-Management um? Was ist die Eintretenswahrscheinlichkeit? Was ist das Schadensausmass?

Kann man IT-Risiken überhaupt bewerten?

Ein grosses Problem beim IT-Risk-Management ist die Risiko-Bewertung. Während man im Risk Management in anderen Gebieten für die Bestimmung der Eintretenswahrscheinlichkeit auf statistische Daten zurückgreifen kann, ist es bei IT-Risiken vielfach nahezu unmöglich, irgendwelche Erfahrungswerte zu bekommen. Zudem kann sich, wie weiter

oben dargestellt, die Eintretenswahrscheinlichkeit sehr schnell ändern.

In vielen Firmen erreicht man eine Pseudo-Genauigkeit, indem man auch «Risiken» im Risiko-Management berücksichtigt, die mehrmals im Jahr vorkommen. Man verkennt, dass Ereignisse, die mehrmals im Jahr vorkommen, eher im Incident-Management-Prozess abzuhandeln sind als in der Risiko-Analyse. Leider werden auch in vielen Lehrbüchern unsinnige Skalen vorgeschlagen, die oft vorkommende Ereignisse mit «wöchentlich» und ein selten vorkommendes Ereignis mit «alle 10 Jahre» kategorisieren. Diese Skala ist in einer IT-Risiko-Analyse unsinnig! Besser wäre, wenn man oft vorkommende Ereignisse mit «jährlich» und selten vorkommende Ereignisse mit «alle 10000 Jahre» gleichsetzen würde. Ein Ereignis, das alle 10000 Jahre eintritt, trifft jedes Jahr eine von 10000 Firmen! Dies dürfte für viele Risiken (z.B. «Grossbrand im RZ»), die man üblicherweise in Risiko-Analysen findet, gar nicht so falsch sein.

Noch schwieriger wird es bei der Bewertung des Schadensausmasses. Falls beispielsweise bei einem Spionageangriff strategische Daten in die Hände der Konkurrenz fallen, dürfte es extrem schwierig sein, den Schaden nur annähernd abzuschätzen. Sehr schwierig sind insbesondere die Reputationsschäden einzuschätzen. Zudem muss berücksichtigt werden, dass sich auch das Schadensausmass eines Risikos schnell ändern kann.

Man kann sich auch durchaus fragen, ob es sinnvoll ist, ein Risiko mit hoher Eintretenswahrscheinlichkeit, aber kleinem Schadensmass in der Kritikalität gleich zu bewerten wie ein Risiko mit einem sehr hohen Schadensausmass und kleiner Eintretenswahrscheinlichkeit.

Diese Schwierigkeiten, die Risiken zu bewerten, führen dazu, dass die Zuteilung zu Klassen bei der Bewertung meistens intuitiv, d.h. ohne explizite Berechnung oder Begründung, vorgenommen wird.

Leben mit Top-Risiken

Bei vielen Firmen gibt es Top-Risiken, deren Eintreten geschäftsbedrohend ist. Häufig ist die Eintretenswahrscheinlichkeit von Top-Risiken schwierig abzuschätzen. Trotzdem müssen diese Top-Risiken bekannt sein und bei allen wichtigen Entscheidungen auf der Geschäftsebene mit einbezogen werden. Vielfach ist es möglich und sinnvoll, Frühwarnsysteme zu etablieren, so dass ein mögliches Eintreten des Risikos im Voraus erkannt werden kann.

Neuere Ansätze im Risiko-Management

Das herkömmliche Risiko-Management basiert auf Annahmen, die im IT-Umfeld häufig hinterfragt werden können. So wird beispielsweise davon ausgegangen, dass die einzelnen Risiken unabhängig voneinander sind. Wie die Katastrophe von Fukushima zeigt, können durchaus Abhängigkeiten vorhanden sein. Dies wird in klassischen Risiko-Analysen nicht berücksichtigt.

Eine weitere Annahme ist, dass das Schadensausmass eines Risikos mit einer gewissen Genauigkeit beziffert werden kann. Es gibt Risiken, bei denen dies möglich ist (z.B. Brand eines Rechenzentrums). Bei anderen Risiken kann das Schadensausmass in einem weiten Bereich variieren (z.B. Verseuchung durch Malware). Soll man nun den maximalen Wert dieses Bereiches einsetzen oder wäre der Mittelwert besser?

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Technik & Architektur
CC Informations- & Softwaresicherheit

Aus den obigen Gründen beginnen sich neuere szenario- und simulationsbasierte Methoden zu etablieren.

Schlussfolgerungen

Es ist unumgänglich, sich beim Betrieb und der Weiterentwicklung einer IT-Infrastruktur von einer Risiko-Analyse leiten zu lassen. Wichtig ist, die konkrete Bewertung jedes Risikos mindestens einmal jährlich neu zu hinterfragen. Diese Bewertung des Risikos sollte von mehreren Spezialisten mit einem breiten Hintergrundwissen durchgeführt werden. Der Einbezug von externen Fachkräften kann dabei sinnvoll sein. Sinnvoll könnte sein, wenn bei der Zusammenstellung des Risikokataloges und der Bewertung des Risikos jedes Jahr Fachkräfte einbezogen werden, die die früheren Risikoanalysen nicht kennen. Wichtig ist, dass sichergestellt werden kann, dass frühere Einschätzungen revidiert werden können. ■

Literatur

- Frank Romeike, KES, August 2010, Artikel «Verdacht: Verkalkuliert».
- Frank Romeike/Peter Hager, Erfolgsfaktor Risikomanagement 2.0, 2. Auflage, Wiesbaden 2009.

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 §