Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 5. Jahrgang, Heft 1, März 2005

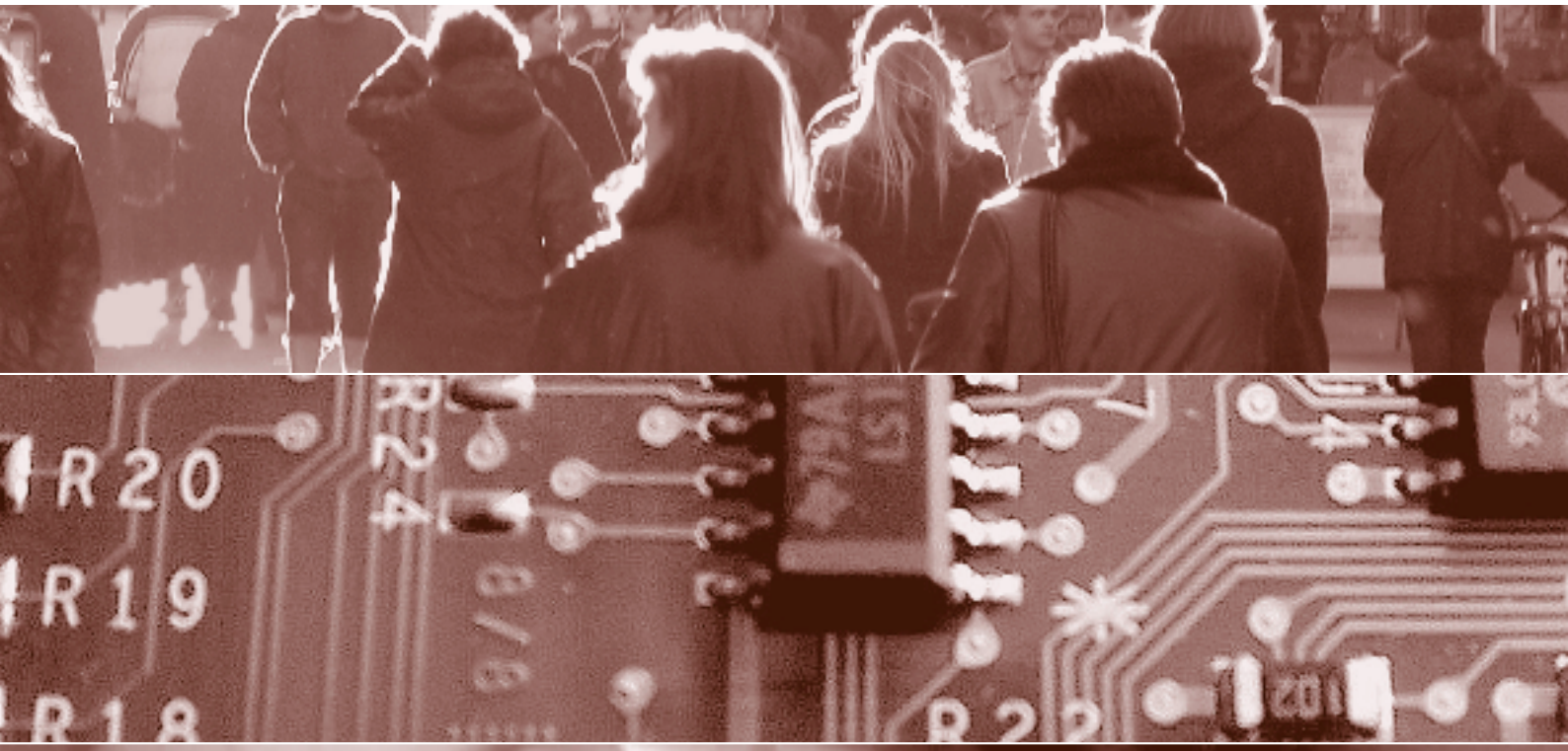
Schwerpunkt:

Pharma

fokus: Biobanken und die Rechte der Spender

fokus: High Performance Computing in Drug Discovery

report: Schutz der Privatheit von «Promis» in Europa



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Michael Waidner

Schulthess §

inhalt

fokus

Schwerpunkt:
Pharma

Ubiquitär vernetzt = ubiquitär unsicher?

Ubiquitäre Netze und Rechner eröffnen interessante Perspektiven. Gleichzeitig entstehen aber auch Sicherheitsrisiken. Security und Privacy müssen integrale und durchgehend gewährleistete Systemeigenschaften werden.

Informationssicherheit im Aussendienst

Das Business geht online, in Zukunft noch stärker als heute. Sobald aber geschäftskritische Daten auf mobilen Geräten gespeichert sind, wachsen auch die Risiken und als Antwort darauf die Sicherheitsanforderungen.

High Performance Computing in Drug Discovery

Bei der modernen pharmazeutischen Forschung entstehen riesige Datenverarbeitungsbedürfnisse. Novartis hat dafür eine High Performance Computing-Strategie mit PC-GRID und DataGRID entwickelt.

Biobanken und die Rechte der Spender

Wer einer Biobank Gewebe und Daten spendet, hat moralische Rechte, die zu berücksichtigen die wichtigste Qualitätsanforderung an eine Biobank ist. Welches sind diese Rechte aus ethischer Sicht?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 13239944, 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. Michael Waidner

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 155.00, Jahresabo Ausland: Euro 126.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Schulthess Druck AG, Esther Cossalter, Arbenzstrasse 20, Postfach, CH-8034 Zürich
Tel. +41 (0)44 386 40 85, Fax +41 (0)44 383 79 45, esther.cossalter@schulthess.com

Druck: Schulthess Druck AG, Bruno Erb, Arbenzstrasse 20, Postfach, CH-8034 Zürich, ISDN +41 (0)44 380 18 86

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

«Sichere» Streichlisten

Streichlisten sollen ausgedient haben, weil sie leicht missbraucht werden können und nicht wirksam vor Phishing-Angriffen schützen. Rolf Oppliger stellt zwei konkrete Möglichkeiten vor, um Streichlisten wirksam vor solchen Angriffen zu schützen.

Schutz der Privatheit von «Promis» in Europa

Das «Caroline-Urteil» des Europäischen Menschenrechts-Gerichtshofes zeigt, wie weit das Privatleben von «Personen der Zeitgeschichte» durch die Europäische Menschenrechts-Konvention gegenüber (Boulevard-)Medien geschützt ist.

Zu Gast in Rapperswil

In der Rubrik «Brückenschlag» beantworten künftig die Experten der Hochschule Rapperswil Technik-Fragen von «Nicht-Technikern» so, dass diese die Antworten auch verstehen.

Weniger Delikte – mehr Angst

Wegen der Kluft zwischen Tatsachen und Wahrnehmung bezüglich Kriminalität befürchten Forscher Auswirkungen auf die Politik. Stephan Russ-Mohl appelliert an die Verantwortung der Medien.

Der Osterhase und die Verhältnismässigkeit

Kinder glauben wider besseres Wissen an den Osterhasen. Der Gesetzgeber tat das auch, als er die Zweifel an der Wirksamkeit der Handy-Registrierpflicht in den Wind schlug. Werden Handys bald besser kontrolliert als Schusswaffen?

In eigener Sache

Mit dieser ersten Nummer des fünften Jahrganges von digma treten zwei personelles Änderungen in Kraft: Die Chefredaktion wird neu abwechslungsweise von Bruno Baeriswyl und Beat Rudin wahrgenommen. Als Rubrikenredaktor für die Rechtsprechung amtet neu Dr. Amédéo Wermelinger, Datenschutzbeauftragter des Kantons Luzern und Lehrbeauftragter an der Universität Luzern.
Herausgeber und Verlag danken herzlich dem scheidenden Chefredaktor, lic. phil. Alex Piazza, der digma sicher und gekonnt durch die ersten vier Jahrgänge gesteuert hat. Ebenso geht der Dank an lic. iur. Marco Fey, der in dieser Zeit die Rubrik Rechtsprechung kompetent betreut hat.

report

forum

Sicherheit in der Praxis

«Sichere» Streichlisten

PD Dr.
Rolf Oppliger,
eSECURITY
Technologies
Gümligen,
rolf.oppliger@
esecurity.ch

Im Internet-basierten elektronischen Geschäftsverkehr spielen Authentifikationsverfahren und -technologien eine wichtige Rolle. Im Einsatz stehen verschiedene Verfahren und Technologien, wie z.B. Passwörter, Transaktionsnummern (in Form von Streichlisten), Einweg-Passwort- und Challenge-Response-Verfahren, sowie Public Key Zertifikate und Smartcards.

Alle Authentifikationsverfahren und -technologien haben Vor- und Nachteile, die es im Hinblick auf eine bestimmte Anwendung zu untersuchen und zu diskutieren gilt. Im Falle von Internet-Banking wird z.B. häufig argumentiert, dass Streichlisten ausgedient haben, weil erstens solche Listen von Aussenstehenden leicht passiv ausgelesen und missbraucht werden können, ohne dass der Benutzer dies merkt, und zweitens Streichlisten nicht wirksam vor Phishing-Angriffen schützen können. Für konventionelle Streichlisten trifft diese Argumentation sicherlich zu und in der Tat können solche Listen aus sicherheitstechnischer Sicht heute kaum mehr empfohlen werden. Dies ist insofern bedauerlich, als es nach wie vor Banken gibt, die zur Authentifikation ihrer Kunden Streichlisten einsetzen, und die nicht kurzfristig auf andere (in der Regel aufwändigere) Authentifikationsverfahren und -technologien migrieren können. Nun gibt es aber Möglichkeiten, Streichlisten zu erweitern und in dem Sinne «sicher» zu machen, dass sie Benutzer vor passivem Auslesen und zum Teil auch vor Phishing schützen.

Schutz vor passivem Auslesen

Wie oben erwähnt, stellt die Möglichkeit, dass Streichlisten von Aussenstehenden passiv ausgelesen werden können, ohne dass der Benutzer dies merkt, ein erstes Sicherheitsproblem dar. Wie kann ein Benutzer z.B. verhindern, dass seine Streichliste von einem Aussenstehenden kopiert wird? Wie kann er feststellen, dass die Liste kopiert worden ist? Wie kann er sicher sein, dass die Liste nicht kopiert worden ist? Die Sicherheit einer Streichliste steht und fällt mit der physischen Sicherheit der Liste. Das Problem stellt sich insbesondere auch vor dem Hintergrund eines möglichen Rechtsstreites. Wird eine Transaktionsnummer missbräuchlich verwendet, kann in der Regel weder der Benutzer noch die Bank den Missbrauch oder die eigene Unschuld nachweisen.

Die Erweiterung, die vor passivem Auslesen schützt, besteht darin, dass man die Transaktionsnummern der Streichliste mit Rubbelfeldern so abdeckt, dass der Benutzer – bevor er eine Transaktionsnummer verwenden kann – das entsprechende Feld auf der Liste freirubbeln muss. Eine Streichliste, deren Transaktionsnummern mit Rubbelfeldern abgedeckt sind, kann nicht mehr unbemerkt passiv ausgelesen werden. Will der Aussenstehende eine Transaktionsnummer in Erfahrung bringen, muss er das entsprechende Feld auf der Streichliste (aktiv) freirubbeln. Dieser Vorgang hat physikalische Einweg-Eigenschaften, d.h. der Vorgang des Freirubbelns kann nicht unbemerkt rückgängig gemacht werden. Wenn mit einer Transaktionsnummer Missbrauch getrieben wird, gibt es grundsätzlich zwei Möglichkeiten: Entweder ist die Nummer freigerubbelt oder nicht. Im ersten Fall hat der Benutzer Erklärungsbedarf; im zweiten Fall die Bank. Verlust der Streichliste ist mit dem ersten Fall gleichzusetzen.

Schutz vor Phishing

Wie ebenfalls oben erwähnt, stellt die Möglichkeit von Phishing-Angriffen ein zweites Sicherheitsproblem dar. Dabei versucht ein Angreifer, mit Hilfe von massenhaft versandten elektronischen Nachrichten und einer gefälschten Web-Site Benutzer zur Preisgabe von persönlichen Authentifikationsinformationen (in diesem Fall Transaktionsnummern) zu verleiten. Zum Teil werden dabei auch sicherheitstechnische Merkmale der graphi-

schen Benutzeroberflächen der Browser mit Hilfe von Skriptsprachen (z. B. JavaScript) so übersteuert, dass Benutzer kaum erkennen können, dass sie mit einer falschen Web-Site verbunden sind.

Im Kern des Phishing-Problems steht die Tatsache, dass die Server-seitige Authentifikation im Rahmen einer SSL/TLS-Verbindung nicht bzw. nicht sorgfältig genug durchgeführt wird. Wenn ein Benutzer eine SSL/TLS-Verbindung zum Internet-Banking-Server aufbaut, authentifiziert sich der Server gegenüber dem Browser des Benutzers mit Hilfe eines Public Key Zertifikates. Das ist theoretisch ein guter Weg. Er geht aber davon aus, dass auf der einen Seite die Ausgabe der Server-Zertifikate seriös gemacht wird, und dass auf der anderen Seite die Gültigkeit der Zertifikate Browser-seitig auch geprüft wird. Genau genommen müsste der Benutzer den Fingerprint des Server-Zertifikates der SSL/TLS-Verbindung mit einem auf anderem Weg von der Bank kommunizierten Wert vergleichen und im positiven Fall noch verifizieren, dass das Zertifikat zwischenzeitlich nicht revoziert worden ist. Das ist in der Praxis zu aufwändig und viele Benutzer vertrauen in der Frage der Gültigkeit von Server-Zertifikaten ihrem Browser bzw. den als vertrauenswürdig vorkonfigurierten Zertifizierungsdiensteanbietern. Wenn es einem Angreifer gelingt, ein Zertifikat von einem solchen Zertifizierungsdiensteanbieter zu erwerben, hat er gute Karten, dass er den Benutzer täuschen und einen «Man-in-the-middle»-Angriff erfolgreich durchführen kann.

Die Erweiterung, die teilweise vor Phishing schützt, besteht darin, dass man auf der Abdeckung der Rubbelfelder (mit den Transaktionsnummern) Codes anbringt, die der Benutzer verifizieren muss, bevor er das Feld freirubbelt. Bei der i.ten Authentifikation wird der Benutzer angehalten, den Code, der vom Server bekannt gegeben wird, mit dem Code auf der Abdeckung von Feld i zu vergleichen und erst im positiven Fall das Feld auch wirklich freizurubbeln. Damit kann der Benutzer den Server zusätzlich zur Server-seitigen Authentifikation im Rahmen einer SSL/TLS-Verbindung authentifizieren.

«Sichere» Streichlisten

Wenn man beide Erweiterungsmöglichkeiten kombiniert einsetzt, kommt man zu «sicheren» Streichlisten, d.h. Streichlisten, die vor passivem Auslesen und zum Teil auch vor Phishing schützen. Die Erweiterungen sind relativ geringfügig und insbesondere auch ohne grössere Investitions- und Betriebskosten realisierbar. Die Erweiterungen betreffen in erster Linie die Herstellung der Streichlisten, sowie die Schulung und Sensibilisierung der Benutzer.

- Bei der Herstellung der Streichlisten sind die Transaktionsnummern mit Rubbelfeldern und entsprechend aufgedruckten Codes abzudecken. Die Codes können mit Hilfe von Pseudo-Zufallszahlengeneratoren und benutzerspezifischen Schlüsseln erzeugt werden.
- Bei der Schulung und Sensibilisierung der Benutzer ist darauf hinzuwirken, dass Transaktionsnummern grundsätzlich nur im Rahmen von vom Benutzer selbst angestossenen Authentifikationsprozessen bekannt gegeben werden, und dass Transaktionsnummern nur dann freigerubbelt werden, wenn der Server einen richtigen (auf dem Aufdruck des Rubbelfeldes vermerkten) Code vorlegen kann.

Man kann davon ausgehen, dass sich mittel- bis langfristig auf dem Markt Streichlisten als Authentifikationsverfahren und -technologie nur dann behaupten können, wenn die beschriebenen (oder ähnliche) Erweiterungen umgesetzt und konsequent eingesetzt werden. Insofern haben Streichlisten im Internet-Banking auch noch nicht ausgedient. ■

Kurz und bündig

Im Internet-Banking wird häufig argumentiert, dass Streichlisten ausgedient haben, weil erstens solche Listen von Aussenstehenden leicht passiv ausgelesen und missbraucht werden können, ohne dass der Benutzer dies merkt, und zweitens Streichlisten nicht wirksam vor Phishing-Angriffen schützen können. In diesem Artikel werden zwei konkrete Möglichkeiten vorgestellt, Streichlisten zu erweitern und in dem Sinne «sicher» zu machen, dass sie Benutzer wirksam vor solchen Angriffen schützen können.