Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 13. Jahrgang, Heft 4, Dezember 2013

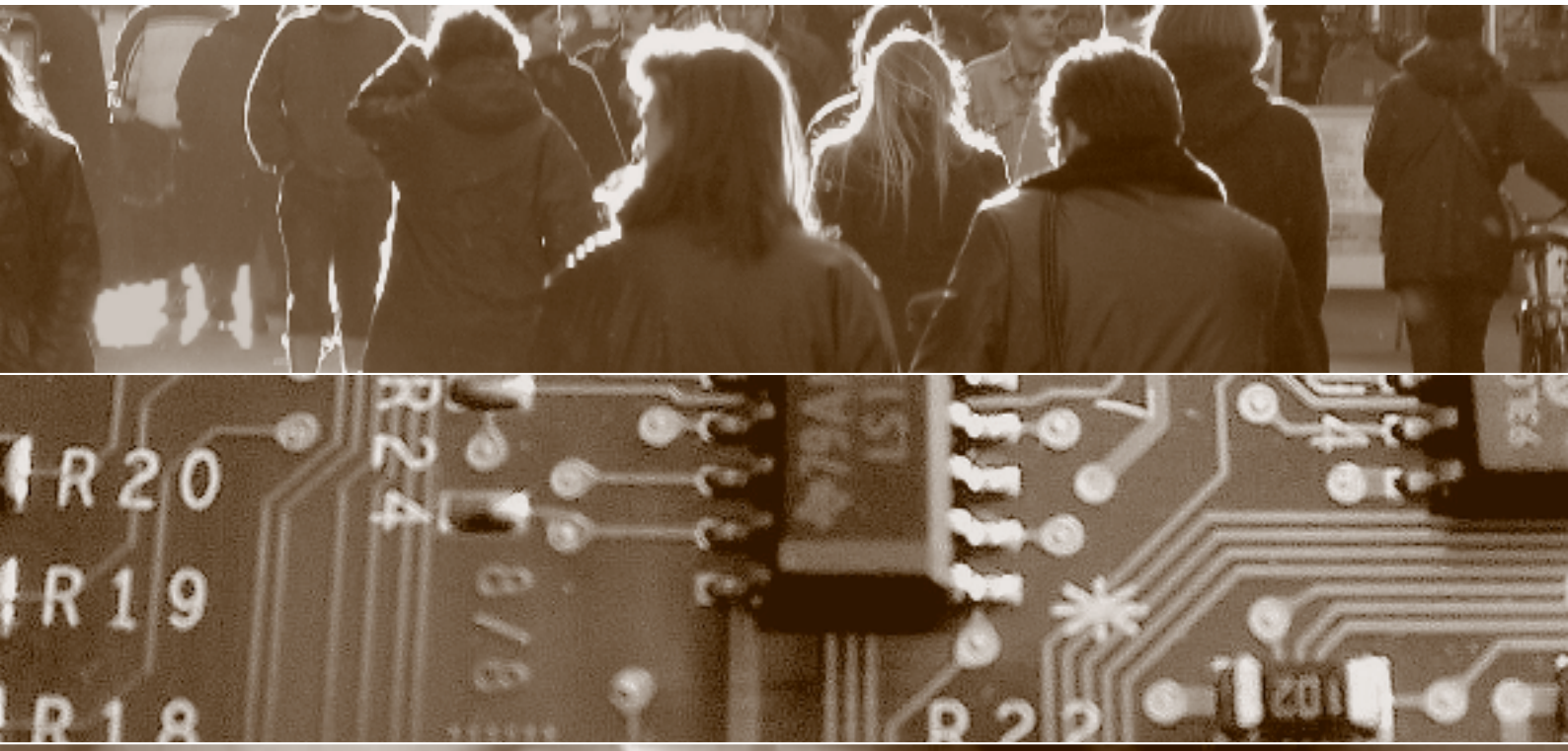
Schwerpunkt:

Best Practice

fokus: Ist «Best Practice» gut genug?

fokus: Zufallszahlen im Dienste der Sicherheit

report: Zur Qualifikation von E-Mails als Urkunde



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

Schulthess §

inhalt

fokus

Schwerpunkt:
Best Practice

auftakt
Demokratie verteidigen im digitalen Zeitalter!
von Writers Against Mass Surveillance Seite 125

Best Practice: Wo sind die Grenzen?
von Bernhard M. Hämmerli Seite 128

Ist «Best Practice» gut genug?
von Hans-Peter Königs Seite 130

«Good Practice» in der Informationssicherheit
von Tom Schmidt/ Maurice Bollag Seite 136

Usability and Security of Today's Passwords
von Kirsi Helkala Seite 138

Föderiertes Identitätsmanagement
von Andreas Spichiger Seite 144

Kryptografische Schlüssellängen
von Tim Güneysu/Andy Rupp Seite 150

Zufallszahlen im Dienst der Sicherheit
von Pavol Svaba Seite 154

Demokratie verteidigen im digitalen Zeitalter

562 namhafte Schriftsteller(innen), darunter Umberto Eco, Günter Grass und Elfriede Jelinek und 19 Autor(innen) aus der Schweiz, protestieren am Internationalen Tag der Menschenrechte gegen Massenüberwachung und fordern eine Internationale Konvention der digitalen Rechte.

Ist «Best Practice» gut genug?

«Best Practice» als die «beste Vorgehensweise» im Vergleich mit anderen vorbildlichen Organisationen oder Handlungsweisen wird oft als Massstab für Organisations-Anforderungen wie Sicherheit, Kontinuität, Datenschutz, Qualität oder Umweltverhalten herangezogen. Doch reicht «Best Practice»?

Usability and Security of Today's Passwords

Das Passwort ist tot, es lebe das Passwort! Passwörter sind nach wie vor die bedeutendste Authentisierungsmethode. Der Bericht zeigt anhand von zwei Studien aus Norwegen auf, unter welchen Voraussetzungen diese Methode weiter verwendet werden kann.

Kryptografische Schlüssellängen

Wann ist Kryptografie als sicher zu erachten? Die EU hat das Network of Excellence EUCrypt finanziert, um aktuelle und fundierte Aussagen für Europa zur Verfügung zu stellen. Der Artikel vermittelt die Grundlagen, um den Fachreport zu interpretieren.

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, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, 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

Die Propheten in der Wüste haben Recht!

Der Dublin-Besitzstand wird weiterentwickelt: In Eurodac verzeichnete Fingerabdrücke sollen neu auch für Strafermittlungen genutzt werden können. Diese Zweckänderung bzw. -erweiterung ist aus rechtstaatlicher Sicht ausgesprochen problematisch.

Zur Qualifikation von E-Mails als Urkunde

Eine Urkundenfälschung begeht, wer eine Urkunde herstellt, deren wirklicher Aussteller mit dem aus ihr ersichtlichen Urheber nicht übereinstimmt. Im Zeitalter der digitalen Kommunikation stellt sich die Frage, ob ein E-Mail eine Urkunde im Sinne des Urkundenstrafrechts darstellt. Die Autoren stellen die bundesgerichtliche Rechtsprechung dar.

Aus den Datenschutzbehörden

Wer ist zur Datenschutzbeauftragten wiedergewählt worden? Wo wurde das Informations- und Datenschutzgesetz um eine Bestimmung zu Pilotversuchen ergänzt? Hier wird über Personelles und Aktuelles aus der Datenschutzszene berichtet.

Überwachungstechnologie unter der Lupe

SurPRISE, finanziert durch das 7. EU-Forschungsrahmenprogramm, prüft auch, ob gewisse Massnahmen, wie etwa Privacy by Design oder juristische Vorkehrungen, es erlauben könnten, Sicherheit mit einem möglichst wirksamen Schutz der Privatsphäre zu vereinen. TA-SWISS führt dazu im März 2014 Diskussionen in der Schweiz durch.

NSA hört mit

Alle sind empört darüber, dass ihnen die NSA überall zuhört. Alle?

report

Dublin-Besitzstand
Die Propheten in der Wüste haben Recht!
von Sandra Husi-Stämpfli Seite 160

Rechtsprechung
Zur Qualifikation von E-Mails als Urkunde
von Lorenz Aenis/
David Mühlemann Seite 164

forum

privatim
Aus den Datenschutzbehörden
von Sandra Husi-Stämpfli Seite 170

Technikfolgenabschätzung
Überwachungstechnologie unter der Lupe
von Christine D'Anna-Huber Seite 172

agenda Seite 173

Tagung
Swiss Cyber Storm Relaunched
von Benjamin Fehrensen Seite 174

schlusstakt
«Euch geht die Arbeit auch nicht aus!»
von Beat Rudin Seite 176

cartoon
von Reto Fontana

Tagung

Swiss Cyber Storm Relaunched



Benjamin Fehrensen, Dr. chem. ETH, Application Analyst, Schroders & Co Bank AG, Zürich
benjamin.fehrensen@swisscyberstorm.com

Swiss Cyber Storm präsentierte sich mit der Nummer 4 erstmals in seinem neuen Gewand. Organisiert und durchgeführt vom hierzu eigens gegründeten Verein «Swiss Cyber Storm», wendet sich die Fachtagung an internationale Sicherheitsspezialisten. Dabei verfolgt sie das Ziel, namhafte Entscheidungsträger und junge ICT-Talente an einer Veranstaltung zusammenzubringen und zu vernetzen.

Während internationale Spezialisten aus Wirtschaft und staatlichen Organisationen referierten, massen sich zehn Finalisten in der Kategorie Studenten an den «Cyber Challenges», um unter sich auszumachen, wer die Schweiz an der «Cyber Alpen Challenge» in Österreich vertreten würde. Die Konferenz stand unter dem Patronat von MELANI (Melde- und Analysestelle Informationssicherung des Bundes) und Swiss Police ITC, einem privaten Verein zur Vernetzung von Strafverfolgung und ICT-Industrie.

Industrialisierung der Spionagesoftware

Eröffnet wurde die Tagung mit der Keynote von Costin Raiu, Direktor des globalen Research & Analysis Team von Kaspersky. Er war mit seinem Team massgeblich an der Analyse des Stuxnet-Wurms, häufig als erste «Cyber Weapon» bezeichnet, beteiligt. Auf Stuxnet im Jahr 2010 folgten Analysen der Schad- und Spionage-Software Duqu 2011 und Flame 2012.

Flame markierte einen Quantensprung in der Entwicklung von Schad-Software. Mittels MD5-Kollisionsattacke war die Spionagesoftware in der Lage, sich mittels gefälschtem Code-Signing-Zertifikat als reguläres Windows-Update zu tarnen und zu verbreiten. Raiu ist überzeugt, dass nur eine Handvoll Leute das notwendige Wissen und den Zugriff auf die notwendigen Ressourcen haben, um eine solch hochentwickelte MD5-Kollisionsattacke durchzuführen.

Wie weit die Industrialisierung im Bereich der Spionagesoftware vorangeschritten ist, verdeutlicht Raiu am selben Beispiel. Flame sei 20 MB gross. Die Software sei bereits dermassen komplex und raffiniert aufgebaut, dass eine vollständige Analyse bis zu zehn Jahre in Anspruch nehmen würde.

Dieser Trend zur Industrialisierung widerspiegelte sich auch in ganz anderen Aspekten. Gemäss Untersuchungen, so Timo Steffens, Vorstand des Nationalen Deutschen IT-Lagezentrums und CERT-Bunds (Abteilungen des BSI, des Bundesamtes für Sicherheit in der Informatik) bestünden Anzeichen dafür, dass gezielte Angriffe in Phasen wie Aufklärung, Infiltration und Datenbeschaffung bzw. Datenabzug unterteilt würden, wobei in jeder Phase unterschiedliche, hierzu spezialisierte Teams zum Zuge kämen.

Sicher ist nur, was nicht sicher ist

Wie viel wissen wir über unsere aktuelle Bedrohungslage? Flame, 2012 entdeckt, enthielt Exploits, die 2008 kompiliert worden waren. Das heisst, vier Jahre lang bestanden massive unentdeckte Sicherheitslücken, ohne dass diese von irgend jemandem entdeckt worden wären.

So kamen in den Diskussionen viele zum Schluss: Mit Sicherheit lässt sich nur sagen, was *nicht* sicher ist. Verlässliche Aussagen darüber, was wie sicher ist, sind hingegen kaum möglich. Genau an diesem Punkt will Thomas Maillart ganz neue Wege beschreiten. Eintrittswahrscheinlichkeiten sollen mittels kalibrierter Modelle, welche mit historischen Daten gefüttert werden, stochastisch vorausgesagt werden. Risiken, die sich quantifizieren lassen, lassen sich auch versichern – so die weiter reichende Überlegung.

Candid Wüest, Virenjäger bei Symantec, zeigte jedoch auf, dass längst nicht alle gezielten Angriffe ausgeklügelte Malware einsetzten. Trotzdem sind die meisten erfolgreich. Von den mehr als hundert täglich registrierten gezielten Angriffen auf Unternehmen zielten letztes Jahr 31% auf KMUs mit weniger als 250 Beschäftigten ab, welche häufig nicht adäquat geschützt sind.

Allerdings macht nicht die Malware den Unterschied zum Massenphänomen, sondern die Person hinter der Malware, welche mit viel Wissen den Angriff steuert.

Diese Ansicht vertrat auch John Matherly, der 2009 die Geräte-Suchmaschine Shodan ins Leben gerufen hat. Matherly zeigte in seinem Vortrag eine von vielen unbeachtete Seite des Internets. Eine immer grössere Flut von «Embedded Devices», kleinen und kleinsten Steuereinheiten in Gebäuden und Geräten, sowie «Mobile Devices» wie Smartphones und Tablets werden direkt mit dem Internet verbunden. Die Anzahl an Mobile und Embedded Devices hat die Anzahl «konventioneller» Webserver schon bei Weitem überschritten.

Leider wird der Sicherheitsaspekt solcher Geräte häufig völlig ausser Acht gelassen. Im Internet finden sich, wie Matherly zeigen konnte, aber nicht nur ungeschützte Küchenmaschinen, sondern auch Haussteuerungen, Windkraftwerke, Wasserkraftwerke, Seilbahnen oder gar ein Krematorium.

Junge Talente herausgefordert

Swiss Cyber Storm hat sich neben seiner Funktion als internationale Fachtagung für IT-Sicherheitsspezialisten gezielt auch die Förderung junger Talente auf die Fahne geschrieben. In dem von Compass Security zur Verfügung gestellten Hacking-Lab konnten sich Schüler und Studenten in den Monaten April/Mai an verschiedensten Aufgaben versuchen und sich hierbei für das Finale qualifizieren.

Jeder der Finalisten sei ein Talent, hob Ivan Büttler, Geschäftsführer von Compass Security in seiner Würdigung der Gewinner hervor. Besonders erfreulich: Ein Finalist erhielt bereits ein Stellenangebot.

It's Cyber Cold War!

In der abschliessenden Podiumsdiskussion, moderiert von Mark Saxer, mit Stefanie Frey, einer der Koordinatorinnen der Umsetzung der Nationalen Cyber-Risiken-Strategie des Bundes, Costin Raiu, Stefan Lüders und dem chinesischen Blogger Michael Anti wurden der jüngst publizierte US-Abhörskandal um PRISM und die Diskussionen um «Cyber War» aufgegriffen. Anti war deutlich: Der Westen habe inzwischen jeden moralischen Vorsprung verspielt. Es fand sich auf dem Podium niemand, der widersprach. Die Diskussion verdeutlichte insgesamt, wie schwierig es ist, auf dem schmalen Grat zwischen Sicherheit und Freiheit Balance zu halten.

Dabei kam auch der omnipräsente, sehr unterschiedlich interpretierte Begriff «Cyber War» ins Spiel. Angesprochen auf die aktuelle Lagebeurteilung kristallisierte sich ein Konsens heraus: «It's Cyber Cold War». Unterschiedliche Konstellationen bedrohen unterschiedliche Ziele auf unterschiedliche Art – aber niemand kann sich die volle Eskalation leisten.

Literatur

http://www.swisscyberstorm.com

Kurz&bündig

«Meet the future talents» war das Motto von Swiss Cyber Storm 4. Im KKL Luzern versammelten sich am 13. Juni arrivierte Entscheidungsträger und Cracks, aber auch junge Talente. Alle gemeinsam verband das Interesse, den Cyberspace sicherer zu machen. Eine Herkulesarbeit, wie die Beiträge der internationalen Sicherheitsexperten aufzeigten. Beendet wurde die Tagung mit einer Podiumsdiskussion, deren Fazit lautetet: «It's Cyber Cold War».

Nächste Nummer

Die nächste Ausgabe von digma erscheint im März 2014 und widmet sich schwerpunktmässig dem Thema **«Schule».**

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 §