Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 15. Jahrgang, Heft 1, März 2015

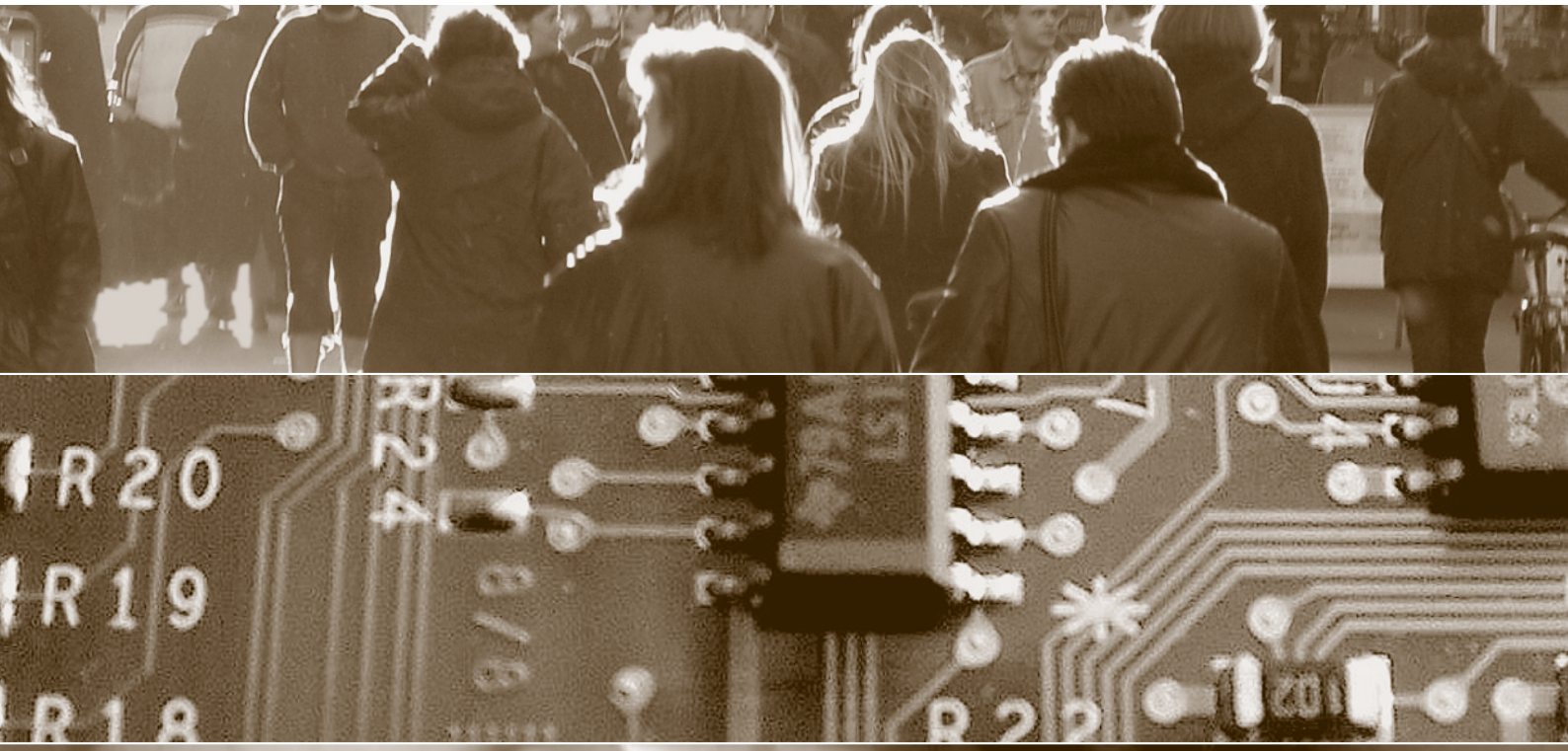
Schwerpunkt:

Klinikinformationssysteme

fokus: Mehr IT-Sicherheit und Datenschutz im Spital

report: Meine Daten machen meinen Preis

report: Widerrechtlich bearbeitete Daten ins Archiv?



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

Schulthess §

inhalt

fokus

Schwerpunkt:
Klinikinformationssysteme

Langer Weg braucht langen Atem

Die Spitäler stehen in der Pflicht, datenschutzgerechte Systeme einzusetzen, die Software-Hersteller sind gehalten, datenschutzkonforme Lösungen anzubieten. Wie können Klinikinformationssysteme datenschutzkonform gestaltet und datenschutzgerecht betrieben werden?

Mehr IT-Sicherheit und Datenschutz im Spital

Die deutschen Datenschutzbeauftragten haben eine «Orientierungshilfe Krankenhausinformationssysteme» verfasst. Das Papier ist mittlerweile in der deutschen Fachöffentlichkeit als Massstab für den datenschutzkonformen IT-Betrieb in Spitälern anerkannt. Wie wird die Orientierungshilfe in Rheinland-Pfalz umgesetzt?

Anforderungen an KIS

privatim hat die wichtigsten technischen Anforderungen an Klinikinformationssysteme (KIS) in einem Dokument zusammengefasst. Der Leiter der Arbeitsgruppe ICT von privatim stellt die wichtigsten Punkte vor.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktorinnen: Dr. iur. Sandra Husi-Stämpfli, Dr. iur. Barbara Widmer

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 Inland: CHF 158.00, Jahresabo Ausland: CHF 183.00, Einzelheft: CHF 42.00
PrintPlus: Jahresabo Inland: CHF 179.00, Jahresabo Ausland CHF 209.00

PrintPlus: Das PrintPlu§-Abonnement bietet die Möglichkeit, bequem und zeitgleich zur Printausgabe jeweils das PDF der ganzen Ausgabe herunterzuladen. Detaillierte Informationen finden Sie unter www.schulthess.com/printplus.

Anzeigenmarketing: Zürichsee Werbe AG, Herr Pietro Stuck, Seestrasse 86, 8712 Stäfa
Tel. +41 (0)44 928 56 11, pietro.stuck@zs-werbeag.ch

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

Meine Daten machen meinen Preis

Der Online-Handel hat schon früh erkannt, welch enormes Potenzial in einer flexiblen Reaktion auf Nachfragekurven liegt. Die Händler sind in der Lage, anhand der Daten, welche die Besucher ihres Webshops hinterlassen, den Preis zu differenzieren und die maximale Zahlungsbereitschaft der Konsumenten individuell abzuschöpfen. Ist Preisdiskriminierung bald allgegenwärtig?

Widerrechtlich bearbeitete Daten ins Archiv?

In welchem Verhältnis stehen Persönlichkeitsrecht (und die daraus entstehenden Ansprüche, z. B. auf Vernichtung widerrechtlich bearbeiteter Personendaten) zu den Dokumentations- und Archivierungspflichten der Verwaltung? Das Verwaltungsgericht des Kantons Bern hat die Frage unmissverständlich beantwortet.

Wenn der Zweck die Mittel heiligen soll

Nach dem Terroranschlag vom Januar 2015 auf «Charlie Hebdo» wurde die Forderung wieder erhoben, dass Fluggastdaten anlassfrei und auf Vorrat erfasst und während fünf Jahren aufbewahrt werden. Der Zweck soll die Mittel heiligen – wie steht diese Forderung zu einem diesbezüglichen Urteil des Europäischen Gerichtshofes? Und was tut die Schweiz?

Die Botschaft les' ich wohl, allein …

Das Bundesparlament will keine stärkere Kontrolle des Nachrichtendienstes, sondern nur eine vorgängige Zustimmung des Bundesverwaltungsgerichts und des Chefs VBS zu heiklen Massnahmen. Soll uns das beruhigen?

Klinikinformationssysteme

Dank den Klinikinformationssystemen stehen Daten über die Patientinnen und Patienten den Pflegenden zur Verfügung. Das soll dazu dienen, die Betreuung der Patientinnen und Patienten zu verbessern. Naja – es kann auch anders herauskommen …

report

forum

Tagungsbericht

Swiss Cyber Storm 2014

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

Swiss Cyber Storm 2014 und das meteorologische Sturmtief Gonzalo fielen dieses Jahr auf den gleichen Tag. Vor beeindruckender Kulisse sprach eine Auswahl internationaler Repräsentanten aus den Gebieten Sicherheitsdienste, Militär und Industrie über die aktuellen Herausforderungen der Computersicherheit, während drei Cyber-Security-Talent-Teams, zusammengesetzt aus Schülern und Studenten, sich im Lösen von Hacking-Challenges massen.

Hyper-embedded und Hyper-connected

Im gleichen Mass, wie die Anforderungen an die heutigen Informatiklösungen steigen, nimmt auch deren Komplexität zu. Moderne Software baut auf vielschichtige Stacks unterschiedlicher Komponenten auf, ganz nach Newtons Weisheit «Wenn ich weiter als andere gesehen habe, dann nur deshalb, weil ich auf der Schulter von Riesen stand». Mächtige Frameworks beschleunigen die Entwicklung. Bestehende Legacy-Komponenten werden eingebunden. Alles wird miteinander vernetzt und durch Schnittstellen erweitert. Eine normale Zahnbürste reicht nicht. Die moderne Zahnbürste kann sich kabellos zu ihrem PC verbinden um Ihnen mitzuteilen, ob Sie oder Ihre Kinder lange genug die Zähne geputzt haben.

All diese Techniken der Softwareentwicklung sind notwendig für den Erfolg: Funktionalität sowie «time to market» müssen stimmen.

Leicht geht bei diesem Hyper-embedding und Hyper-connecting die Übersicht verloren. Worin hat man sich gebettet? Womit ist man vernetzt? Die zeitliche und «digitale Distanz» von «Legacy-Komponenten», teilweise bereits vor 50 Jahren entwickelt, nimmt zu. Software-Komponenten, die ursprünglich für ein geschlossenes System geschrieben wurden, werden plötzlich remote zugänglich.

Die Angriffsoberfläche wird riesig.

Wer soll durch all die Layers noch durchblicken? «Ihre Angreifer haben drei Dinge, die Sie nicht haben: Personal, Geld und Zeit», gibt Patrick Miller, Partner und Managing Principal von The Anfield Group, augenzwinkernd zu bedenken.

Sandworm Vulnerability

Wie einfach das «Einbetten» von Schadsoftware sein kann, zeigt exemplarisch die zurzeit im Internet grassierende Vulnerability Sandworm: Der Exploit versteckt sich in einer Powerpoint Slide-Show (PPSX-Datei). Powerpoint erlaubt das Einbetten von verschiedenen Media-Dateien. Die kompromittierte Powerpoint-Datei enthält zwei «Package Shell Objects». Das eine Objekt verweist auf eine gif-Bilddatei auf einem externen Share. Beim angeblichen Bild handelt es sich jedoch um ein ausführbares Programm. Das andere Objekt entpuppt sich als eine INF-Datei (Setup Information File), normalerweise verwendet, um Meta-Informationen zur Installation eines Treibers mitzugeben. Windows startet, ohne Wissen des Nutzers, automatisch einen Installationsprozess (InfDefaultInstall.exe) um die eingebettete INF-Datei zu verarbeiten. Die INF-Datei weist Windows an, die angebliche gif-Bilddatei umzubenennen und zu starten – der Exploit ist perfekt.

Anti-Hacker-Tool

Die meisten Softwarefirmen zahlen Prämien für Informationen über Sicherheitslücken. Richtig viel Geld wird auf dem Schwarzmarkt geboten. Einige 100 000 Dollar bis zu einer Million, so hört man munkeln, liesse sich auf der «Hacker Tradecraft» (<http://

Weiterführende Literatur

- <http://www.swisscyberstorm.com>

grugq.tumblr.com>) für das exklusive Recht an einem effektiven Zero-Day-Exploit erzielen. Trotz entsprechender Aufrufe habe sich aber noch niemand mit einem Projekt zur Verhinderung von Exploits bei Microsoft gemeldet, beklagt sich Elia Florio, Senior Security Engineer bei Microsoft.

Das im Jahr 2009 ins Leben gerufene Projekt «Enhanced Mitigation Experience Toolkit» (EMET) sammelt innovative Ideen zum Verhindern von Exploits. Das Toolkit zielt darauf ab, das Ausnutzen von Sicherheitslücken möglichst schwierig zu machen, bzw. im besten Fall zu verhindern. Die heute in Version 5.0 vorliegende Software beinhaltet eine ganze Palette von Abwehrmassnahmen wie ASLR (Address Space Layout Randomization), HEAP Protection, NULL Dereference Protection, SEHOP und viele mehr.

Gemäss Elia Florio hätte EMET die Ausnützung einiger der in diesem Jahr entdeckten Zero-Day Attacken verhindern können.

Protection, Detection, Reaction

Die drei Grundpfeiler der Computersicherheit wurden gleich in verschiedenen Vorträgen thematisiert. Bruce Schneiers berühmtes Zitat «It is not prevention or detection, it is response» zielt darauf ab, dass sich viele erfolgreiche Attacken bei rechtzeitiger Intervention hätten vermeiden lassen. Es fehlte nicht an Hinweisen, sondern die angemessene Reaktion blieb aus. Hierbei spielt den Angreifern oft eine falsche Priorisierung der Aufgaben oder eine schlichte Arbeitsüberlastung der zuständigen Administratoren in die Hände. In erhärteten Verdachtsfällen kann es sich durchaus lohnen, rechtzeitig in der Analyse spezialisierte Sicherheitsfirmen hinzuzuziehen. Umfangreiche Log-Korrelation und Auswertung erlauben, Einzelereignisse in einen Zusammenhang zu stellen. Im Falle einer gezielten Attacke, lässt sich ein chronologisches Drehbuch der Abläufe erstellen. Erst das Verständnis, wie eine Attacke abgelaufen ist und auf welche Informationen mögliche Angreifer Zugriff hatten, ermöglicht wirkungsvoll zu reagieren. Insofern wurde die Swiss Cyber Storm auch zur Leistungsshow, wie weit die Techniken in der schnellen Analyse von Big Data ausgereift sind.

Space – Cyberspace

Während Oberst dG Mag. Walter Unger, Colonel (General Staff) des österreichischen Bundesheeres, noch im Jahr 2001 mit einer Handvoll Personen die Abteilung Electronic Defence gegründet hat, ist der Cyberspace mittlerweile zu einem festen Bestandteil geworden, den es zu kontrollieren gilt – gleich wie Land, Luft, Wasser und Weltraum. Die Zeiten, in welchen der virtuelle Raum belächelt wurde, sind vorbei. Die Übergänge der virtuellen und der realen Welt sind allgegenwärtig. So fasste Joseph Nye 2012 die Lage mit folgenden Worte zusammen «Cyberwar, though only incipient at this stage, is the most dramatic of the potential threats.»

Durch die finale Diskussionsrunde führte Tagungsmoderator Mark Saxer, Geschäftsleiter Swiss Police ICT. Die lebhafte Diskussion gipfelte in der Frage: «Was lässt Sie nachts nicht schlafen?». Die Ängste haben sich in den letzten Jahren nicht massgeblich verschoben. Die Verfügbarkeit bleibt Hauptanliegen neben Integrität und Vertraulichkeit.

Cyber Challenges

Ein weiteres Highlight der Tagung sind definitiv die «Cyber Security Challenges». Schüler und Studenten, die sich vorab für den Schweizer Final in Luzern qualifiziert hatten, massen sich im anspruchsvollen Wettkampf auf Zeit. Ivan Bütler, Geschäftsführer von Compass Security, stellte mit seiner Hacking-Lab-Infrastruktur wiederum spannende Aufgaben in einer realistischen Umgebung.

Freuen dürfen wir uns auf die Swiss Cyber Storm 2015:

Vom 20. bis 22.10.2015 wird in Kooperation mit dem EDA und EFD, parallel zur SCS Konferenz, die «European Cyber Security Challenge» neu mit Deutschland, Österreich, Schweiz, Grossbritannien, Spanien und Rumänien durchgeführt. Während SCS-Konferenz und Challenges am 20. bis 21.10.2015 wie üblich im KKL Luzern stattfinden, wird die feierliche Preisverleihung am 22.10.2015 in Bern unter Anwesenheit von Politik, Wirtschaft, Akademia und Militär abgehalten. ■

Kurz&bündig

Zero-Day-Exploits, Advanced Persistent Threats, Forever-Day-Vulnerables: Special Agents, Generäle, Sicherheitsexperten und Studenten tauschen sich aus, was sie nachts vom Schlaf abhält, während drei Cyber-Security-Talent-Teams, zusammengesetzt aus Schülern und Studenten, sich im Lösen von Hacking-Challenges massen.

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 **CHF 183.00** (inkl. Versandkosten)

❑ PrintPlus: Jahresabo Inland **CHF 179.00:** Jahresabo Ausland **CHF 209.00**

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 29
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §