Sicherer Umgang mit sensiblen Daten - technische Prävention und Reaktionen auf Datenschutzverletzungen

Die Diskussion um Maßnahmen zur Verbesserung und Durchsetzung eines angemessenen Datenschutzes rückt durch das stetige Bekanntwerden neuer Datenschutzvorfälle weiter und weiter in die Öffentlichkeit. Dabei kommt medizinischen Daten eine Sonderrolle zu – vor allem angesichts des aktuellen gesellschaftlichen Diskurses zum Thema „Elektronische Gesundheitskarte“ – da ihre Vertraulichkeit wesentlich für das Vertrauensverhältnis zwischen Arzt und Patient ist. Medizinische Daten umfassen unter anderem Art und Umfang der Erkrankung, die Tatsache, dass bzw. ob ein Behandlungsverhältnis bestanden hat, durchgeführte Maßnahmen und Ergebnisse der Untersuchung und natürlich sowie auch alle personenbezogenen Daten. Medizinische Daten sind hoch sensibel und müssen oftmals über einen langen Zeitraum sicher gespeichert werden – teilweise sogar über den Tod des Patienten hinaus. Dies ist insbesondere dann problematisch, wenn aus Kostengründen ein Oursourcing von Aufgaben an dritte Unternehmen erfolgt. Die fehlende Betrachtung von Sicherheitsfragen zeigt beispielhaft der Fall der Deutschen Angestellten-Krankenkasse, die „für die unzulässige Weitergabe von Patientendaten 200.000 chronisch kranker Versicherter an eine Privatfirma, ohne die Versicherten über die Weitergabe zu informieren oder ihre Zustimmung einzuholen“ den BigBrotherAward 2008 erhielt.

Programm

Der ganztägige Workshop findet am 28. September 2009 in vier Sessions à 90 Minuten statt, wobei die vier begutachteten und akzeptierten Einreichungen:

- Wolf, Christopher; Schwenk, Jörg; Wang, Zidu; Jager, Tibor:
  Sicherheitsanalyse von Kreditkarten am Beispiel von EMV
- Baier, Harald; Straub, Tobias:
  Vom elektronischen Reisepass zum Personalausweis:
  RFID und personenbezogene Daten – Lessons Learned!?
- Greveler, Ulrich; Wegener, Christoph:
  Verschlüsselung personenbezogener Daten zur Umsetzung von Löschvorschriften
- Pommerening, Klaus; Sax, Ulrich; Müller, Thomas; Speer, Ronald; Ganslandt, Thomas; Drepper, Johannes; Semler, Sebastian: *Das TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken*

durch die eingeladenen Vorträge:

- Stefan Weiss: *Datenschutzgerechte Betrugs- und Korruptionsbekämpfung in Unternehmen*
- Oliver Raabe: *Datenschutz im Internet der Energie*
- Dominik Birk: *Datenschutz in Sozialen Netzwerken: Freund oder Feind?*
- Markus Engelberth: *Eine Analyse von 33 Gigabyte gestohlener Keylogger-Daten*
- Marit Hansen: *Putting Privacy Pictograms into Practice - A European Perspective*

und eine Paneldiskussion ergänzt werden.

Der Workshop verfolgt dabei die Zielsetzung, wissenschaftliche Beiträge mit Bezug zur technischen Prävention und Reaktion auf Datenschutzverletzungen zu verbreiten und einer fachlichen Diskussion zu unterwerfen. Durch die Hinzunahme der eingeladenen Vorträge wird ein abgerundetes Themenfeld herbeigeführt, das zudem die Möglichkeit bietet, die Referenten und Workshopteilnehmer in einer gemeinsamen Paneldiskussion zum fachlichen Austausch anzuregen. Hierbei können sowohl Besonderheiten der deutschen Datenschutzgesetzgebung selbst als auch fachpolitisch bedeutsame Sicherheitsvorfälle, die sich in Deutschland ereigneten, berücksichtigt werden; dies ist ein unschätzbarer Vorteil der deutschsprachigen GI-Konferenz, der im Rahmen internationaler Informatik-Konferenzen oft nicht gegeben ist.

Beiträge des Workshops

Ohne Zustimmung der Betroffenen kann ein unberechtigter Zugriff auf sensible Daten auch immer dann erfolgen, wenn das zugrunde liegende System Sicherheitsmängel aufweist. Dass dabei mitunter handfeste Geldwerte eine Rolle spielen zeigen Christopher Wolf et al. in ihrer „Sicherheitsanalyse von Kreditkarten am Beispiel von EMV“. Dabei fassen sie Sicherheitsmechanismen moderner Kreditkarten zusammen, zeigen einen möglichen Angriff mittels eines gefälschten Terminals und bieten Möglichkeiten zu dessen Behebung an.

Ebenfalls mit Sicherheitsmängeln und deren Beseitigung mussten sich die Entwickler des für 2010 geplanten elektronischen Personalausweises auseinandersetzen. In ihrem Beitrag „RFID und personenbezogene Daten – Lessons Learned!?“ zeichnen Harald Baier und Tobias Straub die technische Fortentwicklung als Reaktion auf veröffentlichte Schwächen nach und bewerten die Wirksamkeit der getroffenen Maßnahmen im Hinblick auf den Schutz der persönlichen Daten des Inhabers. Weiterhin diskutieren sie, in wieweit der technische und gesellschaftliche Entstehungsprozess von elektronischem Reisepass und elektronischem Personalausweis Modell-Charakter haben kann für die Einführung vergleichbarer Systeme mit kontaktloser Übertragungstechnologie.

Die Einführung des elektronischen Reisepasses wurde durch eine kontroverse Diskussion um den Datenschutz der auf dem Chip gespeicherten personenbezogenen Daten, insbesondere der biometrischen Daten, begleitet. Doch nicht nur biometrische, auch medizinische Daten sind aufgrund ihrer hohen Personalisierung hochsensibel. Dabei gibt es gerade in der medizinischen Forschung, deren Fortschritt in der Regel auch im Interesse des Patienten liegt, deswegen naturgemäß einen Interessenskonflikt zwischen der Weitergabe sensibler Daten an Forschungsgruppen und ethischen Vorstellungen, der ärztlichen Schweigepflicht sowie nationalem und internationalem Datenschutzrecht. Der Beitrag „TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken“ von Klaus Pommerening et al. stellt mit seinem generischen Datenschutzkonzept eine Möglichkeit vor, wie mittels Datentreuhänderdiensten, einem auf Pseudonymen basierendem Identitätsmanagement und Mustervorlagen für Verträge, medizinische Forschung unter Beachtung des Datenschutzes möglich ist.

Einen erweiterten Blickpunkt des Umgangs mit sensiblen Daten in der Unternehmenswelt gibt Stefan Weiss mit seinem Praxisbericht „Datenschutzgerechte Betrugs- und Korruptionsbekämpfung in Unternehmen“. Das Selbstverständnis von Unternehmensvertretern zum Umgang mit den Anforderungen des Datenschutzes wird dabei im Zusammenhang mit erfolgten Betrugs- und Korruptionsbekämpfungsmaßnahmen beleuchtet, bei denen es zu Datenschutzverletzungen gekommen ist. Bei der Betrugs- und Korruptionsbekämpfung in einem Unternehmen geht es zumeist um das Auswerten von Emails, die Analyse der Email oder Telefonkommunikation oder um die Analyse von Verhaltensmustern eines unter Verdacht geratenen Mitarbeiters. Es werden in den meisten Fällen personenbezogene Daten und teilweise auch sensible Daten dazu genutzt, einen Verdachtsfall zu hinterfragen und ggf. Beweise für eine gerichtliche Ermittlung vorzubereiten. In diesem Zusammenhang formuliert die Unternehmensleitung die Einleitung entsprechender Ermittlungs- oder Überwachungsmaßnahmen zumeist mit einem „berechtigten“ Interesse und auch seiner Pflicht, Vermögensschäden vorzubeugen und sich selbst schützen zu müssen. Eine ähnliche Diskussion wird auf Seiten der nationalen Sicherheit in Regierungskreisen geführt und hat oft zur Folge, ein vermeintliches allgemeines Sicherheitsinteresse vor das Persönlichkeitsrecht des Einzelnen zu setzen. Der Praxisbericht soll den Umgang mit diesem Security-Privacy-Paradox anhand aktueller Fälle beleuchten und die Argumentation für die Umsetzung datenschutzkonformer Betrugs- und Korruptionsbekämpfungsmaßnahmen führen.

Nicht nur mit der Berücksichtigung bereits bestehender Regelungen des Datenschutzes sondern auch mit der Frage, ob der bisherige Datenschutz durch Organisationen eine adäquate Antwort auf die Veränderung des klassischen Energiemarktes sein kann, befasst sich der Beitrag von Oliver Raabe. Unter dem Titel „Datenschutz im Internet der Energie“ beschreibt er, wie sich durch neue Übermittlungsverfahren für personenbezogene Messdaten neue Marktrollen und Geschäftsmodelle im Energiemarkt andeuten und zeigt eine Lösung zur möglichen Alternative eines automatisierten Datenschutzes in diesem Bereich auf.

Neben der Veränderung des Energiemarktes spielt das Vertrauen der Nutzer in den rechtskonformen Umgang mit ihren Daten allgemein beim Umgang der Firmen mit Benutzerdaten eine wichtige Rolle. Dazu ist es aber notwendig, dem Benutzer die erfolgende Datenverarbeitung und dabei bestehende etwaige Risiken verständlich zu machen, z. B. indem

diese grafisch visualisert werden. Marit Hansen vergleicht dabei in ihrem Beitrag „Putting Privacy Pictograms into Practice - A European Perspective“ bisherige Ansätze, insbesondere in Bezug auf die europäische Perspektive, leitet entsprechende Anforderungen an sie ab und schätzt Möglichkeiten und Hemmnisse für den Einsatz der Privacy Pictograms im größeren Maßstab ab.

Ebenfalls um das Thema, dem Benutzer eine gute Beurteilung seiner Daten und dem durch die verstärkte Teilnahme an sozialen Netzwerken drastisch steigenden Missbrauchspotential durch Identitätsdiebstahl entgegen zu wirken, geht es bei dem Ansatz von Dominik Birk. Unter dem Thema „Datenschutz in Sozialen Netzwerken: Freund oder Feind?“ diskutiert er die allgemeine Problematik, personenbezogene Daten in sozialen Netzwerken zu veröffentlichen und stellt eine praktische Methode vor, die Kritikalität einer Identität im Internet zu beschreiben.

Dass einmal im Internet veröffentlichte Daten sich in der Regel nicht problemlos wieder löschen lassen, ist mittlerweile unbestritten. Dass dies gerade in komplexen Organisationen mit verteilten Systemen auch der Fall sein kann, da die Umsetzung von Löschvorschriften oft vernachlässigt wird, beschreiben Ulrich Greveler und Christoph Wegener. Durch die Verarbeitung entstehen Kopien von (scheinbar) gelöschten Daten, die nicht mehr ohne erhebliche organisatorische bzw. technische Aufwände durch Löschvorgänge zuverlässig erfasst werden können. Ihr Beitrag „Verschlüsselung personenbezogener Daten zur Umsetzung von Löschvorschriften“ schlägt daher die Verwendung von Verschlüsselung mit späterer Vernichtung der Schlüssel als Ersatz zur technischen Löschung von personenbezogenen Daten im Rahmen eines Löschkonzeptes vor.

Im Gegensatz zu Studien, die auf das beobachtbare Handeln im Verborgenen fokussiert sind, präsentiert Markus Engelberth in seinem Beitrag „Eine Analyse von 33 Gigabyte gestohlener Keylogger-Daten“ einen Überblick über die tatsächlich von Angreifern gestohlenen Güter. Es war den Autoren möglich, etwa 33 GB an Keylogger-Daten zu sammeln und auszuwerten, die von über 173.000 kompromitierten Rechnern stammen.

Danksagung

Die Workshopleitung bedankt sich ausdrücklich bei der Organisation der Konferenz *Informatik 2009* in Lübeck. Die reibungslose Workshopgestaltung wäre ohne die technische und planerische Unterstützung der Konferenzleitung und der technischen Ansprechpartner kaum möglich gewesen.

Workshopleitung

Ulrich Greveler (Fachhochschule Münster)
Pavel Laskov (Universität Tübingen, Fraunhofer FIRST)
Sebastian Pape (Universität Kassel)

Programmkomitee

Ulrich Flegel (SAP Research)
Sandra Frings (Fraunhofer IAO)
Lothar Fritsch (Norwegian Computing Center)
Ulrich Greveler (Fachhochschule Münster)
Marit Hansen (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
Stefan Katzenbeisser (TU Darmstadt)
Pavel Laskov (Universität Tübingen, Fraunhofer FIRST)
Michael Meier (Universität Dortmund)
Holger Morgenstern (IT-Service / Sachverständigenbüro Morgenstern)
Sebastian Pape (Universität Kassel)
Jan Pelzl (escrypt GmbH - Embedded Security)
Kai Rannenberg (Goethe Universität Frankfurt)
Sebastian Schmerl (BTU-Cottbus)
Christian Tobias (Thomas Cook AG)
Stefan Weiss (KPMG)
Christopher Wolf (Ruhr-Universität Bochum)

Organisierende Fachgruppen

FG KRYPTO Fachgruppe für Angewandte Kryptologie
Webseite: http://www.gi-fb-sicherheit.de/fg/krypto/index.html

FG PET Fachgruppe für Datenschutzfördernde Technik
Webseite: http://www.gi-ev.de/gliederungen/fachbereiche/sicherheit/pet.html

FG SIDAR Fachgruppe für Erkennung und Beherrschung von Sicherheitsvorfällen
Webseite: http://www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/