Zeitschrift für Datenrecht und Informationssicherheit

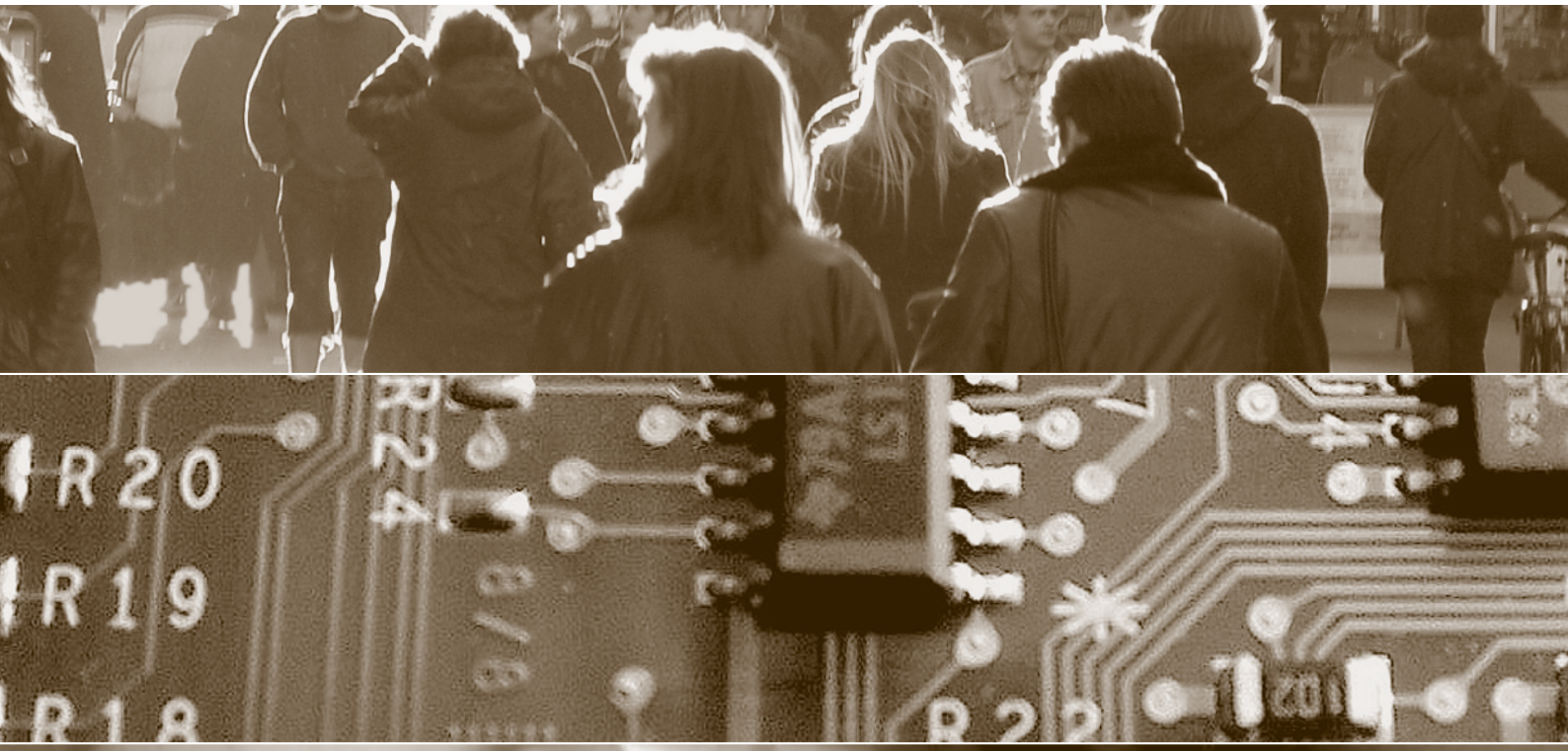
digma

www.digma.info 18. Jahrgang, Heft 2, Juni 2018

Schwerpunkt:

Digitale Demokratie

fokus: E-Voting, ein Mehrwert für die Demokratie
fokus: E-Voting CH: Das Ende der Demokratie?
fokus: Estland im falschen Blickwinkel



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

Schulthess §

inhalt

fokus

Schwerpunkt:
Digitale Demokratie

E-Voting, ein Mehrwert für die Demokratie

E-Voting aus Sicht einer Befürworterin: Es ermögliche die zeit- und ortsunabhängige Stimmabgabe, erfülle strengste Anforderungen, ermögliche den Stimmberechtigten, durch mathematische Verfahren die eigene Stimmabgabe nachzuvollziehen, und gewährleiste den kantonalen Wahlbehörden, jegliche Veränderung im Abstimmungsverfahren erkennen und gegebenenfalls reagieren zu können.

E-Voting CH: Das Ende der Demokratie?

E-Voting aus Sicht eines Skeptikers: Ist es realistisch, darauf zu vertrauen, dass die Bürger bei E-Voting nicht einfach blind der Applikation folgen, sondern den Code überprüfen? Zweifel an der Korrektheit der Abstimmungsergebnisse würden das Vertrauen der Bürger in unseren Staat tief erschüttern.

Estland im falschen Blickwinkel

In staatlichen Digitalisierungs-Strategien wird gerne auf Estland verwiesen. Doch sind die estnischen Erfahrungen unbesehen übertragbar? Auch dort ist die Digitalisierung nicht von der Technologie, sondern durch das Recht gesteuert. Schweizerische Strategien zur Digitalisierung sollten sich deshalb auch an klaren Zielen wie der Stärkung des Rechtstaates und seiner Institutionen, der föderalen Demokratie und der Grundrechte orientieren.

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, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

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

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

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 174.00, Jahresabo Ausland: CHF 199.00, Einzelheft: CHF 48.00
PrintPlu§: Jahresabo Inland: CHF 195.00, Jahresabo Ausland CHF 220.00

PrintPlu§: 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.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa,
Tel. +41 (0)44 928 56 11, pietro.stuck@fachmedien.ch

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Datenkrake Leak-Checker – Lösung in Sicht?

Die existierenden Konzepte zur Information von Betroffenen bei einer Datenschutzverletzung sind ungeeignet, um einen wirklichen Schutz zu bieten. Notwendig ist daher ein neu gedachtes Konzept, dass datenschutzfreundlich arbeitet und dabei proaktiv und umfassend informiert.

Digitalisierung braucht mehr als Feigenblätter

Digitalisierung bringt viel mehr Datenbearbeitungen und damit Risiken für die Grundrechte der Bürgerinnen und Bürger. Sollen die Chancen der Digitalisierung genutzt werden können, müssen die Risiken minimiert werden. Das ist u.a. Aufgabe der Datenschutzbehörden – doch sind sie mehr als Feigenblätter? privatim schlägt Alarm.

Cybersecurity als Bachelor-Studiengang

Der Arbeitsmarkt fordert immer mehr Security-Fachpersonal. Neue Varianten von Informatik-Studiengängen bereiten darauf vor. An der Hochschule Mannheim wird ab Wintersemester 2018/19 ein Bachelor zu «Cybersecurity» angeboten. Seine Interdisziplinarität, spezielle Inhalte zu Automatisierung und ein hoher Praxisanteil sind interessante Aspekte dieses Studiengangs.

Aus den Datenschutzbehörden

Wo wird das Bedrohungsmanagement neu im Polizeigesetz geregelt? Und wo hat das kantonale Verwaltungsgericht die Verwaltungsgerichtsbeschwerde des Datenschutzbeauftragten bezüglich Drohnenaufnahmen in einer Gemeinde gutgeheissen und die Gemeinde angewiesen, sämtliche Luftaufnahmen der betroffenen Grundstücke zu löschen?

Das Stimmgeheimnis beim E-Voting

Die Stimmabgabe nachvollziehbar sicher machen und das Stimmgeheimnis wahren – geht das? Anonym ist verdächtig …

report

forum

Forschung

Datenkrake Leak-Checker – Lösung in Sicht?

Susan Gonscherowski, M.A., Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Deutschland sgonscherowski@datenschutzzentrum.de

Oliver Vettermann, Diplomjurist, FIZ Karlsruhe, Leibniz-Institut für Informationsinfrastruktur, Eggenstein-Leopoldshafen, Deutschland oliver.vettermann@fiz-karlsruhe.de

Versicherungen gegen Datenmissbrauch und Informationsdienste für Betroffene sind eine Antwort auf die grossen Datenschutz-Skandale der letzten Jahre. Genauer hingeschaut ist der Nutzen für die Betroffenen jedoch zweifelhaft. Im Gegenteil: Ein gezielter Blick hinter die Kulissen offenbart, dass beiden Konzepten das Potenzial inhärent ist, selbst «Datenkrake» zu sein. In ihrer jetzigen Form widersprechen sie grundlegenden Anforderungen des Datenschutzrechts nach Transparenz, Datenminimierung wie auch Vertraulichkeit und werden somit selbst zum Risikofaktor für die eigenen Nutzer.

Auswirkungen der DSGVO

Mit der Datenschutz-Grundverordnung (DSGVO) gelten ab dem 25. Mai 2018 in der EU neue Regeln für die Benachrichtigung von Betroffenen nach einem Datenschutzvorfall. Die Vergangenheit zeigt jedoch, dass Datenschutz- bzw. IT-Sicherheitsvorfälle zum Teil erst nach Monaten oder Jahren bekannt werden. Hinzu kommt, dass sensible Daten auf vielfältige Weise, also nicht nur durch grosse Unternehmens-Hacks, sondern auch über gross angelegte Phishing-Kampagnen mit gefälschten Webseiten in die Hände Krimineller gelangen.

Häufig genug helfen die später Betroffenen bei dieser Datenbeschaffung also aktiv mit. Spezialisierte Informationsdienste, sogenannte Leak-Checker, bieten ihren Nutzern die Möglichkeit, durch Eingabe der E-Mail-Adresse zu überprüfen, ob diese Adresse in einem bekannten Daten-Leak enthalten ist. Die Versicherungsbranche entdeckt dieses neue Geschäftsfeld nun auch für sich und bietet ihren Kunden an, sie im Falle einer ungewollten Veröffentlichung personenbezogener Daten darüber zu informieren. Ob und wie viel dann bei tatsächlichem Schadenseintritt gezahlt wird, muss die Zukunft zeigen.

Das vom Bundesministerium für Bildung und Forschung geförderte[1] EIDI-Projekt (= Effektive Information nach digitalem Identitätsdiebstahl)[2] verfolgt das Ziel, die Betroffenen eines Datenlecks, die damit zu potenziellen Opfern eines Identitätsdiebstahls werden, proaktiv, umfassend und besonders datenschutzfreundlich über einen geeigneten Kanal zu informieren.

Im Zuge des Projekts soll ein Software-Framework entworfen werden, welches durch Leaks öffentlich gewordene Identitätsdaten mit denen von Datenverarbeitern (beispielsweise eine Organisation mit Identitätsdatensätzen wie ein soziales Netzwerk) abgleicht und bei positivem Befund die Benachrichtigung des Betroffenen initialisiert. So kann

Literatur, weiterführende Links

- Gonscherowski Susan/Vettermann Oliver, Forschungsprojekt zum digitalen Identitätsdiebstahl, MKWI 2018, 1402 ff., abrufbar unter <http://mkwi2018.leuphana.de/wp-content/uploads/MKWI_152.pdf>.
- Malderle Timo/Wübbeling Matthias/Knauer Sven/Meier Michael, Ein Werkzeug zur automatisierten Analyse von Identitätsdaten-Leaks, Paper zur GI-Sicherheit, 2018, abrufbar unter <https://dl.gi.de/handle/20.500.12116/16293>.
- Roos Philipp/Schumacher Philipp, Botnetze als Herausforderung für Recht und Gesellschaft – Zombies ausser Kontrolle?, MMR 2014, 377 ff.
- Schliesky Utz/Hoffmann Christian/Luch Anika D./Schulz Sönke E. /Borchers Kim Corinna, Schutzpflichten und Drittwirkung im Internet, Baden-Baden 2014.
- Weitere Informationen zum Projekt unter: <https://itsec.cs.uni-bonn.de/eidi/>.

diese – oder auch ein Auftragsverarbeiter – den Identitätsinhaber informieren und schlimmere Folgen für alle Beteiligten abwenden.

An diesem Projekt sind neben der Universität Bonn/Fraunhofer FKIE für die Entwicklung des Frameworks das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) für die datenschutzrechtlichen Fragen sowie für weitere juristische Aspekte das FIZ Karlsruhe (Leibniz-Institut für Informationsinfrastruktur) beteiligt. Darüber hinaus untersucht das Team für allgemeine Psychologie und Kognition der Universität Duisburg-Essen die psychologischen Vorgänge zwischen Information und Nachbetreuung bei einem Identitätsdiebstahl. Durch die interdisziplinäre Aufstellung gelingt eine umfängliche Betrachtung der Thematik, die – wie zu zeigen sein wird – bislang kein ähnliches Modell aufweist.

Unzulänglichkeiten des Versicherungsmodells

Opfer von Identitätsdiebstahl bemerken meist zu spät, dass etwas nicht stimmt. Nämlich in der Regel dann, wenn finanzielle Schäden in Form von Zahlungsaufforderungen oder Reputationsverlust bereits eingetreten sind.

Versicherer werben nicht nur damit, einen finanziellen Schaden zu regulieren, sondern zum Teil auch damit, vor Identitätsdiebstahl zu schützen, indem täglich nach sensiblen Daten der Kunden gesucht und der Kunde im Fall eines bisher unbekannten Fundes benachrichtigt wird. Problematisch hieran sind jedoch die Prozedur und der Umfang der Suche, die bei allen Versicherungen dieser Art ähnlich ist: Die Versicherungen fordern Kunden auf, von ihnen als besonders sensibel erachtete Daten (Reisepassnummer, Adresse, E-Mail-Adresse etc.) einzugeben, und scannen mit diesen dann kontinuierlich «das Internet» ab.

Den Angeboten lässt sich nicht entnehmen, auf welcher technischen Basis die Überprüfung geschieht oder ob und welche bereits bekannten Daten-Leaks enthalten sind. Kritisch zu sehen ist auch, dass sich der Speicherort regelmässig nicht bei der Versicherung, sondern z.T. ausserhalb des Landes bei einem Auftragsverarbeiter befindet. Der Kunde wird zudem nicht darüber informiert, wie lange die gefundenen Daten bei der Versicherung bzw. deren Auftragsverarbeitern gespeichert werden.

Unzulänglichkeiten aktueller Leak-Checker

Aktuelle, öffentlich verfügbare Leak-Checker bieten die Möglichkeit, kostenlos eigene E-Mail-Adressen auf ihr Vorkommen in veröffentlichten Daten-Leaks zu überprüfen. Prominente Beispiele im deutschen Raum sind der Identity Leak-Checker[3] des Hasso-Plattner-Instituts sowie das MELANI Check Tool der zuständigen Schweizer Behörde[4].

Bei Erstem wird die E-Mail-Adresse nach der Eingabe mit dem vorhandenen Bestand an Leak-Daten abgeglichen und der Nutzer anschliessend informiert. Der Weg der Information ist allerdings nicht komplikationsfrei: Aus vorgeblichen Gründen des Datenschutzes wird die Rückmeldung beim Dienst an die eingegebene E-Mail-Adresse gesendet. Bei positivem Fund finden sich in der E-Mail entsprechende Informationen zum Leak bzw. zur möglichen Herkunft des Datenbankeintrags[5]. Der Betroffene wird darüber hinaus, abgesehen von einigen Standard-Verhaltenstipps, nicht weiter beraten. Eine weitere Betreuung fehlt ebenso wie konkrete Handlungshinweise im rechtlichen Bereich (Datenschutzbehörde als Ansprechpartner, Möglichkeiten der Anzeige etc.).

Betrachtet man im Gegensatz den internationalen Leak-Checker «Have I Been Pwned»[6] oder auch das MELANI Check Tool, erfolgt die Rückmeldung dort dagegen unmittelbar im Browser – auch bzgl. verwendeter Passwörter. Wie bei den deutschen Diensten mangelt es ebenfalls an notwendigen Hinweisen.

Mithin ist allen gemein: Es bedarf des aktiven Handelns zum Schutz eigener Daten in der Nachkontrolle. Präventive Aspekte sind nicht ersichtlich. Einzig der amerikanische Dienst bietet ähnlich den Versicherungen einen Informationsdienst an, neuerdings auch in Kooperation mit dem Passwort-Manager 1Password[7].

Kurz&bündig

Betroffene zuverlässig über eine unzulässige Veröffentlichung sensibler Daten und die Gefahr eines Datenmissbrauchs zu informieren, darf nicht länger von der Eigeninitiative der Nutzer abhängig sein. Die existierenden Konzepte sind ungeeignet, um einen wirklichen Schutz zu bieten. Notwendig ist daher ein neu gedachtes Konzept, dass datenschutzfreundlich arbeitet und dabei proaktiv und umfassend informiert. Das hier vorgestellte EIDI-Projekt hat sich diesen Zielen verschrieben.

Matthias Wübbeling, Dipl.-Inf., Universität Bonn, Bonn, Deutschland
matthias.wuebbeling@cs.uni-bonn.de

Timo Malderle, M.Sc., Universität Bonn, Bonn, Deutschland
malderle@cs.uni-bonn.de

Ein neuer Ansatz

Die exemplarisch dargestellten Unzulänglichkeiten existierender Leak-Checker führten zu Überlegungen, insbesondere die Benachrichtigung Betroffener zu verbessern. Vor allem muss dabei die kognitive Verarbeitung der Kenntnis von Daten-Leaks auf der einen Seite wie auch die emotionale Situation des Gewarnten auf der anderen Seite berücksichtigt werden. All das natürlich mit hilfreichen Informationen zu den Daten-Leaks.

Bei allen genannten Leak-Checkern ist es notwendig, dass Personen diesen Dienst bereits kennen und (wiederholt) nutzen müssen, um effektiv von der eigenen Betroffenheit zu erfahren.

Kennt eine Person solche Dienste nicht, so wird sie nur gewarnt, wenn die verantwortliche Stelle sie über in einem veröffentlichten Daten-Leak enthaltene Daten informiert. Um die breite Öffentlichkeit zu schützen, muss also auch für diesen Punkt eine gute Lösung gefunden werden.

Besser ist es, betroffene Personen möglichst zeitnah nach einem Leak selbst, mindestens aber kurz nach einer Veröffentlichung der enthaltenen Daten in entsprechenden Kreisen zu kontaktieren und über notwendige Massnahmen, beispielsweise eine Passwortänderung, zu informieren.

Informationskanal

Obwohl es naheliegend scheint, dem Betroffenen eine E-Mail zu schicken, ist fraglich, ob eine solche E-Mail von den meisten Empfängern nicht eher als Spam-Mail klassifiziert werden wird. Handelt es sich bei den geleakten Daten auch um die E-Mail-Adresse inklusive Passwort, verhindert im Zweifel niemand, dass die Kriminellen eine solche E-Mail einfach löschen, bevor der Betroffene diese überhaupt zu Gesicht bekommt.

Effektiver im Hinblick auf diese Probleme ist es, die Warnung nicht durch den Leak-Informationsdienst selbst zu übermitteln, sondern dafür weitere Kooperationspartner zu nutzen. Diese sind durch die erbrachte Dienstleistung häufig deutlich näher am Nutzer und geniessen ein deutlich grösseres Vertrauen als irgendeine vermeintlich öffentliche Stelle.

Kooperationspartner für ein solches Vorgehen können Web-Dienste (Datenverarbeiter) mit eigener Kundenbindung sein. Hierzu eignen sich also sowohl soziale Netzwerke als auch Online-Shops, rege genutzte Online-Foren oder Spieleplattformen.

Nutzer eines sozialen Netzwerks trauen diesem eher als einem unbekannten Absender einer Warn-E-Mail. Wie sonst wäre zu erklären, dass in sozialen Netzwerken beliebig viele persönliche Daten abgelegt und anderen Personen zugänglich gemacht werden?

Kooperationspartner müssen auch nicht zwingend E-Mails zur Warnung versenden. Vielmehr können Betroffene nach dem nächsten Login durch eine eingeblendete Nachricht informiert werden. So lässt sich zum einen sicherstellen, dass die Informationen tatsächlich bei dem Betroffenen ankommen, zum anderen bietet dies eine interaktive Möglichkeit zur direkten Rückmeldung. Dies ist aber nur eine von mehreren Möglichkeiten von Warnungen ohne E-Mails.

Manche dieser Warnungs-Kanäle benötigen jedoch bestimmte weitere in einem Daten-Leak enthaltene Informationen, um die Warnung an Betroffene eindeutig adressieren zu können. Daher ist es für einen guten Leak-Checker notwendig, gefundene Identitätsdaten selbst möglichst genau zu analysieren, um die enthaltenen Informationen auch zu erkennen. Aufgrund der Vielzahl verfügbarer Daten muss dieser Prozess grösstenteils automatisch erfolgen.

Gesetzliche Grundlage

Betrachtet man die eingangs aufgezeigten Unzulänglichkeiten, scheint es, als bleibe der Bürger als Grundrechtsträger in digitaler Hinsicht nahezu ungeschützt zurück. Wenngleich das deutsche Bundesverfassungsgericht in seinen Entscheidungen zum Allgemeinen Persönlichkeitsrecht und der wegweisenden Entscheidung zur Informationellen Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG feststellte, es gebe kein belangloses Datum[8], so fehlt es bislang an einer gesetzgeberischen Gewährleistung des effektiven Schutzes im digitalen Raum. Die erläuterte proaktive Verhaltensweise wird nur mässig dem gerecht, wozu der Gesetzgeber kraft seiner Schutzpflichten imstande und verpflichtet ist.

Lediglich interessierte und bereits ausreichend sensibilisierte Personen nutzen das vorhandene Angebot regelmässig; das Interesse am deutschen Pendant zum MELANI Check Tool – dem BSI-Sicherheitstest – führte unmittelbar nach Bekanntwerden zu einer Überlastung der Website[9].

Ob das blosse Bereithalten ein zugleich angemessenes Mittel darstellt, kann ebenfalls infrage gestellt werden. Mithin sind in diese Betrachtung die Umsetzung und der Erhalt des Datenschutzniveaus einzubeziehen. Die vertiefte Prüfung, inwieweit eine Schutzpflicht des Staates zum Schutze der digitalen Identität vorliegt, ist im Rahmen des eingangs er-

wähnten Projektes vorgesehen. Im Moment kann aber festgehalten werden, dass der Gesetzgeber kraft deutschem Verfassungsrecht aus dem Allgemeinen Persönlichkeitsrecht[10] – genauer: der Informationellen Selbstbestimmung und dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[11] – zum Schutz der digitalen Identitäten der Bürger verpflichtet sein kann. Insoweit käme das Software-Framework des EIDI-Projektes der notwendigen Prävention und Nachbetreuung des digitalen Identitätsdiebstahls nach.

Technische Umsetzung

Zunächst gilt es zum jetzigen Zeitpunkt eine exemplarische Umsetzung zu erstellen, die in der Lage ist, Betroffene von Identitätsdaten-Leaks zu informieren, ohne selbst eine riesige Sammlung personenbezogener Daten vorzuhalten und somit lohnenswertes Ziel für Hacker zu werden. Ein wesentliches Merkmal ist dafür die Information ohne proaktives Interesse potenziell Betroffener. Hierfür müssen sowohl eine zweifelsfreie Identifikation auf Basis der vorliegenden Daten möglich sein – handelt es sich ja schliesslich bei Daten-Leaks um personenbeziehbare Daten – als auch neue Kommunikationskanäle geschaffen werden, die eine direkte Ansprache erlauben.

Dafür setzt das EIDI-Projekt auf Kooperationen zwischen öffentlichen und privaten Organisationen. Eine öffentliche Einrichtung mit der Aufgabe, die Bürger im Cyberspace zu schützen, könnte dann selbst oder in einer Public-Private-Partnership solche öffentlich verfügbaren Identitätsdaten sammeln. In Kooperation mit Datenverarbeitern könnte dann zum Beispiel die Person hinter einer E-Mail-Adresse oder einem bestimmten Dienste-Konto identifiziert werden.

Bei einem sozialen Netzwerk liesse sich an einen Hinweis beim nächsten Anmeldevorgang des Nutzers denken. Ein Online-Shop hat dagegen in den meisten Fällen auch noch Zugriff auf eine Postadresse, so dass auch zusätzliche oder alternative Kommunikationswege (wie ein klassischer Brief) genutzt werden können, um die Person darüber zu informieren, dass persönliche Daten von Kriminellen genutzt werden.

Selbstverständlich erfolgt der Austausch zwischen all diesen Stakeholdern unter Berücksichtigung der aktuellen Gesetzeslage möglichst datensparsam. Es werden also nicht einfach E-Mail-Adressen im Klartext zum Datenabgleich übertragen, sondern mittels etablierter Hash-Funktionen berechnete Zeichenketten (Pseudonyme). Diese erlauben es dem Datenverarbeiter nicht, die Daten selbst beliebig zu nutzen, aber ermöglichen dennoch einen Abgleich mit seinem eigenen Datenbestand. Dies gelingt, da auf beiden Seiten gleichermassen verhashte Daten (gleiche Pseudonyme) vorliegen, indem sich zuvor über die Hash-Funktion und notwendige Parameter (z.B. individueller SALT) geeinigt wird. Entscheidend ist, dass nur die Pseudonyme in Klartext auflösbar sind, die sowohl im Daten-Leak als auch beim Datenverarbeiter vorliegen. Betroffene, die der Datenverarbeiter nicht kennt, bleiben ihm damit weiter unbekannt.

Wichtig ist im nächsten Schritt der psychologische Aspekt des Forschungsprojekts, nämlich die Ansprache und weitere Begleitung der betroffenen Personen. Hier ist sicherlich zu beachten, dass «Oma Erna» anders angesprochen werden muss, als ein 20-jähriger «Digital Native». Insbesondere das Verständnis der Abläufe eines Daten-Leaks und die möglichen Folgen digitalen Identitätsdiebstahls sowie sinnvolle Vorgehensweisen wie ein Passwort-Wechsel, ein Tausch der E-Mail-Adresse

Fussnoten

1 BMBF-Förderschwerpunkt: Erkennung und Aufklärung von IT-Sicherheitsvorfällen, abrufbar unter: <https://www.forschung-it-sicherheit-kommunikationssysteme.de/>.
2 <https://itsec.cs.uni-bonn.de/eidi/>.
3 Abrufbar unter: <https://sec.hpi.de/ilc/search>.
4 Abrufbar unter: <https://checktool.ch/>.
5 Siehe hierzu insb. <https://sec.hpi.de/ilc/publickeys>.
6 Abrufbar unter: <https://haveibeenpwned.com/>.
7 Abrufbar unter: <https://1password.com>.
8 Siehe BVerfGE 65, 1 (45).
9 Vgl. Philipp Roos/Philip Schumacher, MMR 2014, 337 (378).
10 Zu den daraus folgenden Schutzpflichten siehe auch Di Fabio Udo, in: Maunz Theodor/Dürig Günter, GG-Kommentar (81. EL), Art. 2, Rn. 189 f; Schliesky/Hoffmann/Luch/Schulz/Borchers, Schutzpflichten und Drittwirkung im Internet (2014), 119 ff.
11 Hierzu nur BVerfGE 120, 274 (302 ff).
(Alle URL letztmals kontrolliert am 28.5.2018.)

oder der eigenen Telefonnummer sollten dann ebenfalls thematisiert werden. Dafür wird die Wirkung von verschiedenen Kommunikationswegen, Ansprachen und Warnungsformen untersucht.

Um nicht selbst Opfer von Hackern zu werden und damit weitere Daten-Leaks zu verhindern, werden die Daten nach einer Warnung für die weitere Verwendung unkenntlich gemacht. Spezielle Hashverfahren erlauben dann zwar noch die Überprüfung, ob zum Beispiel für eine E-Mail-Adresse bereits eine Warnung versendet wurde, allerdings ist die E-Mail-Adresse selbst nicht mehr auf den Systemen gespeichert. Gerade dies ist ein wichtiger Schritt zu einem zuverlässigen und datenschutzkonformen System zum Schutz einer breiten Öffentlichkeit in Deutschland. ■

agenda

23. Symposium on Privacy and Security
Stiftung für Datenschutz und Informationssicherheit
6. September 2018, Zürich
http://www.privacy-security.ch

Sommerakademie 2018: Beschäftigtendatenschutz im digitalen Zeitalter
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
10. September 2018, Kiel
https://datenschutzzentrum.de/sommerakademie/2018/

40th International Data Protection and Privacy Commissioners Conference
22.–26. Oktober 2018, Brüssel
http://www.privacyconference2018.org/

digma-Tagung zum Datenschutz: Datenschutz in der täglichen Praxis von Städten und Gemeinden
Schulthess Forum
14. November 2018, Zürich

42. Datenschutzfachtagung (DAFTA) und 37. RDV-Forum
Gesellschaft für Datenschutz und Datensicherheit (GDD)
14.–16. November 2018, Köln
https://www.gdd.de/seminare/dafta

21. Berner Tagung für Informationssicherheit
ISSS
23. November 2018, Bern
https://www.isss.ch

Computers, Privacy and Data Protection (11th International CPDP Conference)
30. Januar–1. Februar 2019, Brüssel
http://www.cpdpconferences.org/

Nächste Nummer

Die nächste Ausgabe von digma erscheint im September 2018 und widmet sich schwerpunktmässig dem Thema **«Cybersouveränität».**

Schulthess §

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

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

Sprache: deutsch

☑ **JA,** ich profitiere vom **Mini-Abo** von **digma** und erhalte **2 Ausgaben** zum Kennenlernpreis von nur **CHF 58.–** (inkl. MWST und Versandkosten).

Vorname/Name

Firma

Strasse/Nr.

PLZ/Ort

E-Mail

Datum/Unterschrift

Abonnement-Bedingungen

Wenn ich digma danach weiterlesen möchte, muss ich nichts weiter tun und erhalte im Jahresabonnement 4 Printausgaben zum Preis von CHF 174.00 (inkl. MWST, zzgl. CHF 6.00 Versandkosten). Falls ich digma nicht weiter beziehen möchte, melde ich mich spätestens 7 Tage nach Erhalt der 2. Testausgabe bei Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich, E-Mail: service@schulthess.com, Fax: +41 (0)44 200 29 28.

A

Nicht frankieren
Ne pas affranchir
Non affrancare

Geschäftsantwortsendung Invio commerciale-risposta
Envoi commercial-réponse

Schulthess Juristische Medien AG
Kundenservice
Zwingliplatz 2
Postfach 2218
8021 Zürich