Forschungsprojekt EIDI

Effektive Information nach digitalem Identitätsdiebstahl

DELIVERABLE 2.8.1

Datenschutz und Identitätsschutz-Modelle

ausgearbeitet von

Susan Gonscherowski

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

MIT UNTERSTÜTZUNG VON JAROSLAW PEKAL UND SILKE MÜLLER

UNIVERSITÄT DUISBURG-ESSEN - ALLGEMEINE PSYCHOLOGIE: KOGNITION

Kiel, im November 2018

Projektpartner

RHEINISCHE FRIEDERICH-WILLHELMS UNIVERISÄT BONN

Informatik 4

Friedrich-Ebert-Allee 144
53113 Bonn

Prof. Dr. Michael Meier
0228 7354249
mm@cs.uni-bonn.de

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Holstenstr. 98
24103 Kiel

Harald Zwingelberg
0431 98812222
uld6@datenschutzzentrum.de

LEIBNITZ-INSTITUT FÜR INFORMATIONSINFRASTRUKTUR GMBH KARLSRUHE

Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldhafen

Prof. Dr. Franziska Boehm
07247 808555
franziska.boehm@kit.edu

UNIVERSITÄT DUISBURG-ESSEN

Allgemeine Psychologie: Kognition

Forsthausweg 2
47057 Duisburg

Prof. Dr. Matthias Brand
0203 3792541
matthias.brand@uni-due.de

XING AG
Dammtorstraße 30
20354 Hamburg

Förderhinweis

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 16KIS0697 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Redaktionsschluss: November 2018

Kurzfassung

Ziel dieser Untersuchung war die Auswertung bestehender Identitätsschutz-Modelle – auch Leak-Checker genannt – in Bezug auf die Einhaltung datenschutzrechtlicher Vorgaben. Untersucht wurden sechs verschiedene Modelle. Drei Modelle nutzen einen kontenbasierten Ansatz. Hier legt der Nutzer ein eigenes Profil an und befüllt verschiedene Kategorien, wie Adressen, Kontakt- oder Bankdaten mit eigenen Daten. Der Dienst überprüft dann, ob diese Daten irgendwo im Internet verfügbar sind. Werden entsprechende Daten gefunden, informieren die Dienste ihre Nutzer darüber.

Die anderen drei Modelle verfolgen einen ereignisbasierten Ansatz. Hier kann der Nutzer nach Bedarf überprüfen, ob seine E-Mail-Adresse in einem bekannten Leak enthalten und ob ggf. weitere Datenkategorien betroffen waren. Ein Profil bzw. eine Anmeldung ist nicht notwendig. Der Nutzer erhält jedoch keine Benachrichtigung im Falle eines neuen Vorfalls sondern muss selbstständig tätig werden.

Die Vor- und Nachteile der einzelnen Modelle wurden herausgearbeitet und fließen in die Entwicklung des EIDI-Frameworks mit ein. Im Sinne des Datenschutz-by-Design-Ansatzes sollen die Fehler der bestehenden Modelle vermieden und durch datenschutzfördernde Ansätze ersetzt werden.

Inhaltsverzeichnis

1 Individuum und Identität

Name und Ziel des EIDI-Projekts ist die „Effektive Information nach digitalem Identitätsdiebstahl“. Aber warum stellt ein Identitätsdiebstahl überhaupt ein Problem dar und wer soll mit welchem Ziel unterrichtet werden? Um diese Fragen zu beantworten, ist es erforderlich sich mit der Bedeutung von Identität für ein Individuum auseinanderzusetzen.

In diesem ersten Abschnitt sollen daher grundlegende Fragen aus dem Themenkomplex Identität aufgegriffen werden. Ebenso wird die Beziehung zwischen Individuum, Umwelt und Identität betrachtet. Als unsere Annahme im Rahmen der Betrachtung sei an dieser Stelle vorweggenommen: das Individuum mit einer bestimmten Identität existiert nicht (mehr).[1]

1.1 Eine kurze Geschichte der Identität

Die erste tatsächliche Verwendung des Begriffs ‚Identität‘ ist zurückzuführen auf das 17.Jahrhundert, als der Philosoph und Vordenker John Locke in seinem Essay über das menschliche Verständnis die Identität der Person als das Selbst bezeichnete welches denkende Individuen voneinander unterscheidet.[2] So lässt bereits die Ableitung des Begriffs Identität aus dem lateinischen Wort ‚idem‘, welches für ‚derselbe‘ steht, darauf schließen, dass die Identität den wesentlichen Teil einer selbstgewählten, aber auch durch soziale Interaktionsprozesse durch die Umwelt geformten Persönlichkeit darstellt. George Herbert Mead wählte daher eine kategorische Differenzierung in eine soziale und personale Identität.[3] Die soziale Identität bezeichnet dabei die Zugehörigkeit zu einer sozialen Gruppe wie einer Nation, Religion, Kultur aber auch einer Familie. Unter der personalen Identität werden alle Teil-Identitäten subsummiert, welche neben den gesellschaftlichen Einflüssen dem Individuum eigen sind. Dazu zählen körperliche Merkmale wie der Fingerabdruck, der Klang der Stimme, die Körpergröße aber auch der Grad der Intelligenz. Gleichzeitig interagiert die Identität in sozialen Gruppen und definiert dadurch das Zugehörigkeitsgefühl. Gerade die Ich-Identität, wie sie bereits durch Siegmund Freud geprägt wurde, ist das Ergebnis aus einer Vielzahl von Interaktionen mit dem Umfeld und letztlich das Bild, welches der Mensch selbst über sich hat und andere Menschen über einen haben. Es ist ein Maßstab für die Erwartungshaltung gegenüber anderen und sich selbst und dient als Orientierungshilfe für Ent-

[1] S. Storch: Identität in der Postmoderne – Mögliche Fragen und mögliche Antworten, über: http://zrm.ch/images/stories/download/pdf/publikationen/publikation_storch_19990101.pdf (abgerufen am 06.07.18).
[2] Locke, John (1981 [1690]): *Versuch über den menschlichen Verstand*, Band 1, Hamburg: Felix Meiner Verlag.
[3] Mead, George H., (1968 [1934]): *Geist, Identität und Gesellschaft*, Frankfurt am Main: Suhrkamp. Im Original: (1934): Mind, Self, and Society, Chicago: The University of Chicago Press.

scheidungen und Verhaltensweisen. Das soziale Selbst bedarf neben der Interaktion mit Individuen auch deren Anerkennung. Der Soziologe Charles Horton Cooley ging noch einen Schritt weiter und begründete die These, dass die Bildung einer Identität in höchstem Maße von anderen Individuen abhängig ist, da das resultierende Selbst-Gefühl aus den Urteilen, Rückmeldungen und Erwartungen anderer entspringt.[4] George Herbert Mead griff diese Idee etwas später auf und fasste das Identitätsbild damit zusammen, dass die Identität den Blick mit den Augen der anderen auf einen selbst darstellt.[5] Einen entscheidenden Beitrag in der Identitätsforschung leistete auch Erik Erikson, der der Identität eine gewisse Verletzlichkeit zusprach, da er im Gefühl des Ichs die Aufrechterhaltung von Kontinuität und Einheitlichkeit sah.[6] Ein Konstrukt, bei der ein Eingriff diese Einheitlichkeit ins Wanken bringen und das subjektive Vertrauen in die Wahrung von Kontinuität verletzen könne. Die Unterteilung in eine soziale und eine personale Identität lässt sich ebenfalls auf die digitale Repräsentation des Selbst übertragen: Benutzernamen, Passwörter, Emailadressen und Kontodaten können einem spezifischen Individuum zugeordnet werden. Sie sind zwar veränderbar, repräsentieren aber dennoch eine einzelne digitale Identität. Da wir mit Hilfe der Medien ein digitales Abbild unseres Selbst und damit auch eine Identität schaffen – unabhängig davon in wie weit diese Repräsentation tatsächlich unserem realen Ich entspricht –, wird diese digitale Identität in hohem Maße angreifbar. Die spezifischen Personenmerkmale sind damit nicht länger nur ein innerer Teil von uns, sondern liegen verstreut auf vielen unterschiedlichen Servern, und damit außer Reichweite einer vollen eigenständigen Kontrolle. Ein digitaler Identitätsdiebstahl ist damit nicht nur mit einem materiellen Schaden verbunden, sondern kann sich als ein schwerwiegender Einschnitt in das subjektive Vertrauen zur Wahrung der Kontinuität einer persönlichen Identität erweisen.

1.2 Zwischenfazit

Ein Identitätsdiebstahl kann ein sehr einschneidendes Erlebnis sein. Die Art und Weise, wie ein Individuum von der Außenwelt wahrgenommen wird, wird durch einen Identitätsdiebstahl stark beeinflusst. Durch einen Identitätsdiebstahl werden die Interaktionsprozesse zwischen Individuen und deren Umwelt gestört. Der Mensch als soziales Wesen (zoon politikon)[7] ist von diesen Prozessen in höchstem Maße abhängig. Die Selbstverwirklichung des Einzelnen ist nur möglich durch das Zusammenspiel mit der Gemeinschaft.[8]

---

[4] Cooley, C. H. (1956): *The Two Major Works of Charles H. Cooley: "Social Organization" [1909] – "Human Nature and the Social Order" [1902]*; introd. by Angell, R., Glencoe, Illinois: The Free Press; S. 168-210.

[5] Mead, G. H., (1968 [1934]): *Geist, Identität und Gesellschaft*, Frankfurt am Main: Suhrkamp. Im Original: (1934): Mind, Self, and Society, Chicago: The University of Chicago Press.

[6] Erikson, E. H. (1979 [1959]): *Identität und Lebenszyklus*, Frankfurt am Main: Suhrkamp.

[7] Siehe Höffe, O.(Hrsg): Aristoteles - Politik, 2. Aufl. (2011), Akademie Verlag.

[8] Siehe Lersch,: Der Mensch als soziales Wesen. Eine Einführung in die Sozialpsychologie, 2. Aufl. 2013, S. 13.

Der Identitätsbegriff wie er im EIDI-Projekt angewendet wird, erschöpft sich hingegen in der Dimension der digitalen Identität sowie einigen wenigen sozialen Teil-Identitäten eines Individuums. Identität im Sinne des EIDI-Projekts muss technisch abbildbare Merkmale vorweisen können. Hier schließt sich der Kreis zu den digitalen Identitäten, welche im Dokument D 2.4 umfassend beschrieben werden, die genau diese Bedingung erfüllen.[9]

Dieses Spannungsverhältnis ist die Crux. Die Opfer eines Identitätsdiebstahls sehen sich häufig mit den Folgen dieses Vertrauensbruchs konfrontiert ohne nachvollziehen zu können, wie es dazu kam. Die Verletzung der von Erikson postulierten Einheitlichkeit führt zu einer Verzerrung zwischen Außen- und Innenwahrnehmung der Identität und verhindert damit letztendlich die Selbstverwirklichung des Betroffenen. Im Begriffskanon der Grundrechte ist dies ein Eingriff in die verfassungsmäßig garantierte Handlungsfreiheit, die letztlich auch die Würde des Menschen tangiert (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Das Bundesverfassungsgericht entwickelte hierfür - mit Blick auf die elektronische Verarbeitung personenbezogener Daten – eigens den Begriff der informationellen Selbstbestimmung.[10] Daraus folgt, dass das Problem eines Identitätsdiebstahls darin besteht den Betroffenen in seiner (unantastbaren) Menschenwürde zu verletzen und mittels dieser Behandlung zumindest gefühlt zu einem Objekt herabzustufen.

Ziel eines Identitätsschutzmodells sollte daher sein, diese Verletzung zu verhindern. Ob und wie dies gelingt wird im Folgenden analysiert werden. Keinesfalls sollte das verwendete Verfahren selbst das Risiko einer Verletzung von ähnlicher Tragweite wie ein Identitätsdiebstahl mit sich bringen.

2 Ansatz der Risikobewertung

Die Rolle, die eine digitale Identität für das Individuum spielt und die unter anderem daraus beeinflusste Abschätzung der Risiken im Falle eines Datenmissbrauchs im Zusammenhang mit dieser Identität, sollte nicht nur subjektiv durch den Einzelnen erfolgen, sondern durch objektive Kriterien ermittelt werden. Ausgehend von den Modellen zum Schutz digitaler Identitäten (unten Kapitel 3) soll eine erste Einteilung verschiedener Warnstufen konzipiert werden. Für eine erfolgreiche Warnung der Betroffenen ist es zwingend erforderlich, dass diese eine Benachrichtigung ernst nehmen. Die bestehenden und hier analysierten Modelle (unten Kapitel 4) setzen bei der Risikobewertung zum großen Teil auf die Einschätzung des

[9] Bruegger, B.: Datenschutzrelevante Merkmale digitaler Identitäten (D 2.4), März 2018.
[10] Siehe BVerfGE 65, 1 (Volkszählung).

Betroffenen und damit eine subjektive Sichtweise. Eine objektive Beurteilung des Risikos ist auf diese Weise unwahrscheinlich.

Das Risiko einer Datenverarbeitung unter datenschutzrechtlichen Gesichtspunkten ergibt sich grundsätzlich aus der Schwere des Eingriffs in die Rechte und Freiheiten natürlicher Personen und der Wahrscheinlichkeit mit der sich ein potentielles Risiko in einem tatsächlichen Schaden manifestiert.[11] Das Recht auf informationelle Selbstbestimmung, das durch jede Form der Verarbeitung personenbezogener Daten beeinträchtigt wird, steht regelmäßig im Fokus der Risikoanalyse.[12] Die Beschränkung hierauf würde jedoch zu einer verzerrten Einschätzung führen. Die Verarbeitung personenbezogener Daten kann für eine Vielzahl von Rechte und Freiheiten zum Risiko werden, z.B. für die freie Meinungsäußerung, das Recht auf Eigentum oder Gesundheit. Inwieweit eine Beeinträchtigung gegeben sein kann, ist jeweils anhand des konkreten Verarbeitungsverfahrens zu beurteilen. Neben dem Risiko eines immateriellen Schadens durch Eingriffe in Rechte und Freiheiten, sind auch Risiken materieller Schäden in die Beurteilung einzubeziehen.[13] Nachdem eine mögliche Beeinträchtigung ausgemacht wurde, ist zu klären, wie intensiv diese ist. Die Intensität lässt sich nicht konkret beziffern sondern nur mittels Klassen unterteilen. Die Eingriffsintensität verstärkt sich abhängig von Art, Umfang, Zweck und Umständen der Verarbeitung.[14] Diese können sowohl einzeln als auch kumulativ wirken und erhöhen die Eingriffsintensität sukzessive auf hoch bis sehr hoch.[15]

Der zweite Faktor zur Bestimmung des Risikos ist die Eintrittswahrscheinlichkeit. Jede Verarbeitung personenbezogener Daten, also Erhebung, Speicherung, Verwendung etc. stellt zunächst einen Eingriff in die informationelle Selbstbestimmung des Betroffen dar. Die Eintrittswahrscheinlichkeit liegt damit nahezu bei 100 %. Lediglich die Intensität des Eingriffs kann variieren. Die Eintritts Wahrscheinlichkeit für andere Eingriffe oder Schäden hängt maßgeblich vom Verarbeitungsprozess bzw. vom Verfahren ab. Das folgende Beispiel soll die Differenzierung der Faktoren und Variablen veranschaulichen:

> Bob möchte in den Urlaub nach Spanien fliegen. Bei der Buchung des Tickets werden Bobs personenbezogene Daten in Form von Name, Geburtsdatum, Personalausweisnummer, Kreditkarteninformation und Buchungsnummer verarbeitet. Die Buchungsnummer ist der Identifikator der Bob innerhalb der Fluggesellschaft zu einem bestimmten Ticket (Abflugs- und Zielort, Zeit, Sitzplatz im Flugzeug) zuordnet.

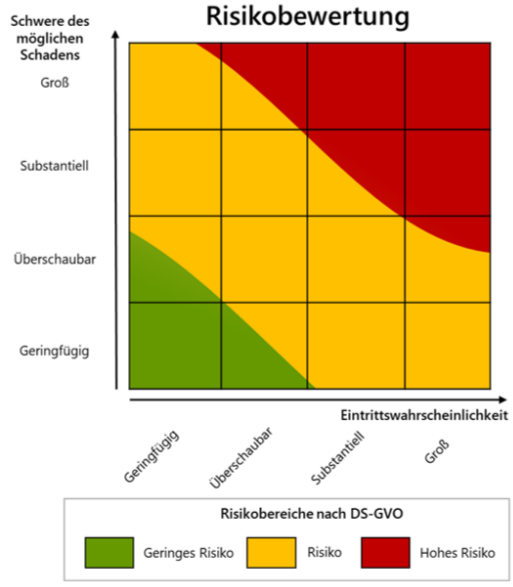
---

[11] Vgl. Bieker: Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, in: DuD, 1/2018, S. 29.
[12] Martini in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 24 DSGVO Rn. 28-30.
[13] DSK: Kurzpapier Nr. 18, über: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_18_Risiko.pdf (07.11.2018), S. 5.
[14] Martini in: Paal/Pauly, Art. 24 DSGVO Rn. 31-35a.
[15] Vgl. Bieker: Die Risikoanalyse, S. 30.

Name, Geburtsdatum und Personalausweisnummer verifizieren mit hinreichender Sicherheit am Check-In, dass Bob wirklich Bob ist und die Kreditkarteninformation ist für die Bezahlung des Tickets erforderlich. Bis hierhin beschränkt sich der Eingriff in Bobs Recht auf informationelle Selbstbestimmung auf ein vertretbares (normales) Maß. Der Eingriff ist zweckgebunden und verhältnismäßig, das Risiko ist entsprechend normal.

Werden Bobs Daten jedoch auf einer No-Fly-Liste vermerkt, ändert sich das Risiko, denn nun ist nicht nur Bobs Recht auf informationelle Selbstbestimmung durch den Eintrag auf dieser No-Fly-Liste **zusätzlich** beeinträchtigt (zusätzliche Datenverarbeitung zu einem anderen Zweck). Auch in sein Recht auf Freizügigkeit gemäß Art. 11 GG bzw. Art. 45 EuGrCH wird hierdurch eingegriffen - nämlich dann, wenn Bob aufgrund des Eintrags in dieser Liste nicht wie geplant fliegen darf, weil ihm der Zutritt zum Flugzeug verwehrt wird. Steht Bob zu Unrecht auf der No-Fly-Liste der Fluggesellschaft, z.B. wegen eines Fehlers, entsteht ihm einerseits ein immaterieller Schaden (Eingriff in die Freizügigkeit). Andererseits kann Bob auch die gebuchte Dienstleistung nicht in Anspruch nehmen und ihm entsteht hierdurch ein finanzieller (materieller) Schaden.

Abb. 1 Risiko



Das Beispiel verdeutlicht die kumulative Wirkung auf das Risiko, die eine Erweiterung der Verarbeitung personenbezogener Daten bewirken kann. Die Zweckerweiterung über die ursprüngliche Datenverarbeitung hinaus führt zu einem zusätzlichen Risiko für die Rechte und Freiheiten des Betroffen. Die Risikobewertung ist daher für jede Stufe einzeln zu bewerten.

Die Klassifizierung des Risikos kann in drei Stufen erfolgen. Die Datenschutzaufsichtsbehörden bezeichnen diese als *gering, normal* und *hoch* (Abb. 1)[16]. Das Standarddatenschutz-Modell leitet das Risiko – in Anlehnung an die Grundschutz-Methodik des BSI – aus dem Schutzbedarf ab. Da der Schutzbedarf *normal, hoch* und *sehr hoch* sein kann, ist folglich auch das Risiko *normal, hoch* oder *sehr hoch*.[17] Da der Schutzbedarf jedoch auch die Eingriffsintensität beschreibt, handelt es sich hierbei ledig-

[16] DSK: Kurzpapier Nr. 18, S. 5.
[17] AK Technik: SDM, S. 31 f.

lich um eine formale und nicht um eine inhaltliche Differenz.[18] Die DSGVO verwendet die Begriffe *Risiko* und *hohes Risiko* und lässt die Bezeichnung der dritten Klasse ganz offen.

In Erwägungsgrund 76 DSGVO heißt es hierzu ausdrücklich: „Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt." Aus der Objektivitätsanforderung folgt, dass die Risikoeinschätzung für jedermann nachvollziehbar sein sollte. Entsprechend transparent ist die Art und Weise der Risikobeurteilung zu gestalten, damit auch der Betroffene die Beurteilung verstehen kann. Dies gilt insbesondere, wenn für die Beurteilung des Risikos, wie bei meineSCHUFA, auf einen Algorithmus zurückgegriffen wird.[19]

Ebenso wenig reicht es für ein Identitätsschutzmodell aus, die bloße Betroffenheit eines Nutzers festzustellen. Dies fördert zwar die Transparenz in Bezug auf den stattgefundenen Datenmissbrauch, versetzt die Betroffenen jedoch nicht in die Lage angemessen zu handeln, da diese in den meisten Fällen nur ihren eigenen subjektiven Maßstab anlegen können. In der Folge kann dies zu einer Fehleinschätzung der Situation führen.

3 Modelle zum Schutz digitaler Identitäten

Internetkriminalität ist längst zum Risikofaktor in vielen Lebensbereichen geworden. Mit der Zeit haben sich am Markt unterschiedliche Ansätze herausgebildet um diesem Risiko zu begegnen. Die meisten dieser Identitätsschutz-Modelle zielen darauf ab, dass der Nutzer Kenntnis davon erlangt, dass sensible Daten in Umlauf geraten sind. Weiß der Nutzer bereits, dass Daten durch Kriminelle missbraucht werden, stellt sich die Frage, was dagegen unternommen werden kann. Mittlerweile sind verschiedene Ansätze von unterschiedlichen Anbietern verfügbar und es stellt sich, insbesondere vor dem Hintergrund des Datenschutzrechts, die Frage, ob es sich hierbei um Angebote handelt, die tatsächlich das Risiko eines Identitätsdiebstahls senken können. Darüber hinaus muss auch die Verarbeitung personenbezogener Daten im Rahmen der angebotenen Dienstleistung den Anforderungen des Datenschutzes genügen und sollte für die Betroffenen nicht zum Risiko werden.

Hierzu erfolgt im Abschnitt 3.1 zunächst ein Überblick über und eine Differenzierung der Begriffe Identitätsdiebstahl, Identitätsbetrug sowie Identitätsbezogene Kriminalität um den

[18] So auch Bieker: Die Risikoanalyse, S. 30.
[19] Vgl. Rost: Künstliche Intelligenz, in: DuD 9/2018, S. 561.

eigentlichen Zweck der Identitätsschutz-Modelle rechtlich einordnen zu können. Die Fokussierung auf Identitätsdiebstahl in der Analyse der unterschiedlichen Angebote soll eine Vergleichbarkeit zwischen den verschiedenen Modellen ermöglichen.[20]

In Abschnitt 3.2 werden die Beurteilungskriterien, die der Analyse zu Grunde liegen erläutert. Ziel ist es eine objektive Beurteilung in Bezug auf die allgemeinen Anforderungen des Datenschutzes vornehmen zu können und die verschiedenen Ansätze gegeneinander abzuwägen. Abschnitt 3.3 enthält die Einzelanalysen der betrachteten Konzepte, die sich jeweils in eine Beschreibung des Konzepts und die sich daraus ergebenden Schlussfolgerungen in Bezug auf die Beurteilungskriterien. Die Ergebnisse der Analyse werden in Abschnitt 3.4 zusammengefasst.

3.1 Begriffsdefinitionen

3.1.1 Identitätsdiebstahl

Eine Legaldefinition des Begriffs „Identitätsdiebstahl" existiert im deutschen Recht nicht. Der Begriff wird daher je nach Kontext unterschiedlich weit verstanden.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) definiert Identitätsdiebstahl als Vortäuschung einer falschen Identität durch einen Angreifer.[21] Der Angreifer verwendet häufig identifizierende Merkmale einer anderen Person zur Verschleierung der eigenen Identität, um sich dann im Namen dieser Person zu bereichern oder andere Straftaten zu begehen. Grundsätzlich ist die Begehung dieser Taten aber auch möglich in dem der Täter sich eine neue – nicht existierende Identität – erschafft. Hierbei fehlt dann jedoch der „Sündenbock", der zunächst mit den Taten in Verbindung gebracht wird. Der Vorteil der Nutzung einer bestehenden Identität liegt für den Angreifer insbesondere darin, dass durch die Verwendung der Identität eines anderen jeglicher Verdacht zunächst auf diese Person gelenkt wird. Das verschafft dem Angreifer vor allem Zeit um einerseits weitere Straftaten zu begehen und andererseits unbemerkt sowie unerkannt unterzutauchen.[22]

[20] Anmerkung: Aus Datenschutzsicht muss es soweit gar nicht erst kommen, denn die Veröffentlichung sensibler Daten im Internet ist, wie auch ein Identitätsdiebstahl, bereits ein Folgeschaden eines Datenschutzvorfalls und damit einer Verletzung der Rechte der Betroffenen.

[21] Siehe BSI: IT-Grundschutz G 0.36 Identitätsdiebstahl, über: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g00/g00036.html (abgerufen am 04.07.18).

[22] Siehe Leenes: ID-related Crime: Towards a Common Ground for Interdisciplinary Research (D5.2b), über: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf (abgerufen am 10.07.2018), 59 f.

Aus (datenschutz-)rechtlicher Sicht können personenbezogene Daten, da sie keine Sachen im Sinne des Gesetzes sind, per se nicht gestohlen werden. Insofern ist der Begriff des Identitäts*diebstahls* irreführend, denn wo keine Sache ist, kann auch keine „entwendet" werden. Die Tatbestandsmerkmale des § 242 Abs. 1 StGB sind damit nicht erfüllbar.

3.1.2 Identitätsbetrug

Synonym zum Identitätsdiebstahl wird teilweise der Begriff „Identitätsbetrug" verwendet. Einen Betrug begeht nach § 263 Abs. 1 StGB:

> *„Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält […]".*

Diese Legaldefinition enthält im Gegensatz zu der des Diebstahls Merkmale, die mit denen des Identitätsdiebstahls bzw. –Betrugs laut BSI übereinstimmen. Allerdings beschränkt sich das Strafrecht in der Begriffsdefinition des Betruges auf einen Vermögensschaden. Immaterielle Schäden, wie die Persönlichkeitsrechtsverletzungen oder Rufschädigung, können hierrüber nicht geltend gemacht werden. Dies ist lediglich über den zivilrechtlichen Weg (z.B. Schadenersatz nach § 823 BGB) möglich.

Je nach Kontext in dem die personenbezogenen Daten missbraucht werden, geht der Identitätsbetrug in verschiedenen – strafrechtlich bewährten – Tatbeständen auf. Hierzu gehören beispielsweise Waren- und Kreditbetrug, Urkundenfälschung, Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung oder Beleidigung.

Der Begriff des Identitätsbetrugs bedarf im Hinblick auf die aktuellen technischen Entwicklungen möglicherweise einer neuen Definition – als jemanden um seine Identität betrügen, oder genauer um eine Teilidentität. Diese Auslegung würde sich an der Bedeutung des Wortes Identität orientieren und zielt in eine der Definition von Koops und Leenes entsprechende Richtung.

3.1.3 Identitätsbezogene Kriminalität?!

Koops und Leenes schlagen den Terminus „identity-related crime"[23] (Identitätsdelikte/identitätsbezogene Straftaten/identitätsbezogene Kriminalität) als übergeordneten Begriff vor. Die Autoren begründen dies damit, dass der neue Begriff jeden unrechtmäßigen Gebrauch einschließt, der Identitäten zum Ziel hat oder diese als Werkzeug missbraucht.[24] Dies umfasst nicht nur den Wechsel und die Nutzung einer fremden Identität bzw. die Erschaffung einer Neuen sondern auch die Zerstörung einer Vorhandenen oder auch die Wieder-

[23] S. Koops/ Leenes: Identity Theft, Identity Fraud and/or Identity-related Crime, in DuD 9/2006, S. 554.
[24] Vgl. Koops/ Leenes: Identity Theft, Identity Fraud and/or Identity-related Crime, in DuD 9/2006, S. 554.

herstellung/Wiederbelebung einer stillgelegten Identität. Gleichzeitig sollen legitime Zwecke von einer Kriminalisierung ausgenommen sein.[25] Dies ist insbesondere dann von Bedeutung, wenn aus Datenschutz- oder anderen legitimen Gründen die wahre Identität einer Person nicht offenbart werden soll/darf bzw. nicht gewünscht ist. So ändert ein Journalist zum Schutz des Informanten beispielsweise dessen Namen im Artikel, ein Blogger wählt sich ein Pseudonym unter dem sie/er veröffentlicht oder ein Unternehmen ordnet nach einem Mitarbeiterwechsel eine Funktions-Adresse einer anderen Person zu. Sollen nach Abschluss einer medizinischen Studie die Ergebnisse veröffentlicht werden, müssen die Daten anonymisiert werden, d.h. die für eine Studie erstellte Teilidentität wird dadurch zerstört.

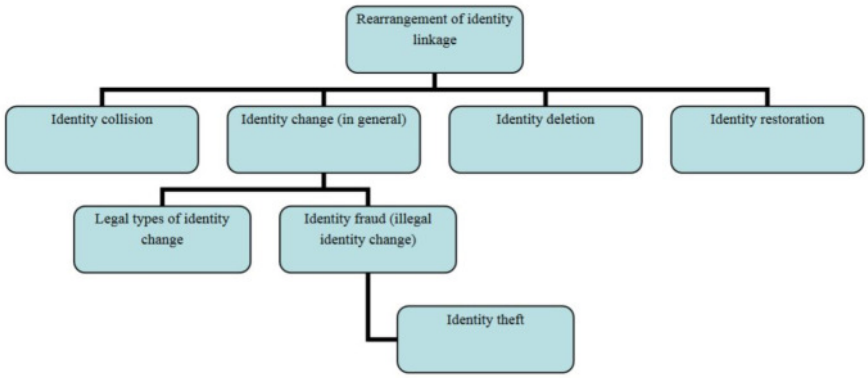
Leenes leitet eine Differenzierung zwischen Identitätsdiebstahl und Identitätsbetrug aus der Verbindung zwischen Teilidentität und identifizierenden Merkmalen (Identifier) ab.[26]

Identitäten bestehen nicht nur für natürliche Personen sondern auch für Organisationen. Denkbar ist demnach auch, dass Identitätsbetrug mit Identitäten juristischer Personen begangen wird. CEO-Fraud basiert beispielsweise darauf. Hierbei tritt ein Angreifer als Vertreter bzw. Organ einer Organisation (juristischen Person), z.B. Geschäftsführer oder Vorstandsmitglied, gegenüber einem Mitarbeiter auf und fordert diesen beispielsweise zur Anweisung eines größeren Geldbetrages auf ein ausländisches Konto auf.[27] Auf ganz ähnliche Weise funktionieren auch Phishing-Mails[28] und andere Betrugsmaschen in denen der Angreifer sich als Behörde, Bank oder auch Nachlassverwalter[29] ausgibt und den Empfänger unter einem Vorwand dazu verleitet sensible Daten preiszugeben.

Leenes argumentiert daher, dass Identitätsdiebstahl einen Spezialfall des Identitätsbetrugs darstellt. Identitätsbetrug wiederum gehört zur Kategorie der Identitätswechsel (s. Abb. 2)[30]. Die Hauptkategorie bildet die Neuzuordnung einer Identität

[25] Siehe Leenes: ID-related Crime, Kap. 4.
[26] Vgl. Leenes: ID-related Crime, S. 48.
[27] BKA: Warnhinweis CEO-Fraud, über: https://www.wirtschaftsschutz.info/DE/Themen/Wirtschaftskriminalitaet/PDFCEOFraudbka.pdf?__blob=publicationFile&v=7 (abgerufen am 04.07.18).
[28] Vgl. Leenes: ID-related Crime, S. 66.
[29] Europäisches Verbraucherzentrum Deutschland: Vermeintliche Erbschaft, über: https://www.evz.de/de/verbraucherthemen/vorsicht-falle/vermeintliche-erbschaft/ (abgerufen am 04.07.18).
[30] Vgl. Leenes: ID-related Crime, S. 56.

Abb. 2 Identitätsbegriffe nach Leenes



Ein Identitätswechsel zeichnet sich dadurch aus, dass eine Person absichtlich eine Änderung einer Identität herbeiführt.[31] Leenes beantwortet außerdem die Frage, warum Identitätsdiebstahl ein wachsendes Problem ist. Er führt dies auf eine ungünstige Konstellation aus schwachen Authentisierungsverfahren und im Verhältnis dazu weitreichenden Rechten einer Identität im jeweiligen Kontext zurück.[32] Grundsätzlich entsprechen solche Authentisierungsverfahren den Standards in menschlichen Interaktionssystemen: Wenn jemand jemanden wiedererkennt, z.B. einen Freund, ist die Person damit zu bestimmten Handlungen oder Äußerungen autorisiert beispielsweise dazu Informationen aus dem Privatleben des Freundes zu erfahren. Dies kann zu der Annahme verleiten, diese Muster ließen sich auf digitale Identitäten übertragen. Erkennt beispielsweise jemand ein Profil anhand eines Profilbildes und/oder des Profilnamens wieder und verfährt dann nach dem oben genannten Muster, indem intime private Dinge preisgegeben werden, werden Autorisierungen angenommen, die bezogen auf den Kontext „soziales Netzwerk“ nur durch eine sehr schwache Authentifikation gestützt werden, denn grundsätzlich kann sich jeder mit jedem beliebigen Bild und Namen dort anmelden. Wird dieser Irrtum wissentlich aufrechterhalten, handelt es sich um Identitätsbetrug.

Identitätsbetrug im soziologischen Kontext bedeutet nach Leenes: „[…]to claim the fulfilment of someone else‘s legitimate expectations concerning one‘s own identity, role and behaviour within a specific communicational context, but to only simulate the others‘ expectations towards them, and thus to evade these expectations deliberately.“[33]

Diese Ansicht greift bereits einen Kerngedanken auf der von Datenschützern immer wieder betont wird und auch in das europäische Datenschutzrecht aufgenommen wurde. Es genügt nicht, aus Datenschutzverletzungen resultierende Schäden einzugrenzen. Vielmehr muss bereits von den Verantwortlichen alles dafür getan werden, dass digitale Identitäten vor identitätsbezogenen Straftaten geschützt werden. Datenschutz durch Technikgestaltung und

[31] Vgl. Leenes: ID-related Crime, S. 51.
[32] Vgl. Leenes: ID-related Crime, S. 46-48 und 59.
[33] Leenes: ID-related Crime, S. 55.

datenschutzfreundliche Voreinstellungen sind wirksame Werkzeuge auch zur Prävention von Identitätsbetrug und fester Bestandteil einer sicheren Verarbeitung. Da es jedoch keine 100 %ige Sicherheit gibt, könnten Identitätsschutzmodelle das Repertoire der Schutzmaßnahmen sinnvoll ergänzen.

3.2 Kriterien und Modelle

In diesem Kapitel sollen verschiedene, aktuell bestehende Modelle zum Schutz digitaler Identitäten näher untersucht werden. Ausschlaggebend für die Bewertung der Modelle ist, wie datenschutzfreundlich diese gestaltet sind. Maßstab hierfür sollen wiederum die sieben Gewährleistungsziele des SDM sein.[34] Die Kriterien an die Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nichtverkettung und Datenminimierung für Identitätsschutzmodelle werden im Folgenden erläutert. Sie leiten sich aus den generischen Anforderungen, wie sie im SDM beschrieben sind ab.

3.2.1 Datenminimierung

Obwohl ein wesentlicher Bestandteil von Identitätsschutzmodellen die Datenerhebung ist, gilt auch hier der Grundsatz der Datenminimierung.[35] Dieses Grundprinzip ist ausdrücklich in Art. 5 Abs. 1 lit. c) DSGVO genannt. Die angewandten Methoden sollten sicherstellen, dass die betriebene Datenverarbeitung zielgerichtet erfolgt. Die Zwecke der Verarbeitung – also der Schutz oder die Warnung vor einem Identitätsdiebstahl – sollten mit der geplanten Verarbeitung erreicht werden können.[36] Der Erforderlichkeit der Daten wird die Beschränkung der Datenverarbeitung „auf das erforderliche Maß“ beigestellt. Damit ist nicht nur eine den Inhalt beschränkende sondern auch eine die Dauer der Verarbeitung (zeitliche) Komponente vorgesehen.[37] Die Speicherbegrenzung wird in Art. 5 Abs. 1 lit. e) DSGVO präzisiert.

Es sollte zunächst festgelegt werden, welche Daten überhaupt für einen Identitätsdiebstahl verwendet werden könnten bzw. welche Angriffsszenarien in diesem Kontext überhaupt möglich sind. Hier sind durchaus unterschiedliche Ansätze denkbar, die sich in entsprechend unterschiedlichen Angeboten wiederspiegeln. Im Zuge dessen sind die von Art. 25 DSGVO geforderten Maßnahmen festzulegen. Sowohl auf technischer wie auch auf organisatorischer Seite sollte sichergestellt werden, dass nur das Minimum an notwendigen Daten für einen bestimmbaren Zeitraum verarbeitet wird.[38] In der Regel werden die getroffenen Maßnahmen durch weitere Maßnahmen im Sinne des Art. 32 DSGVO abzusichern sein.

---

[34] Vgl. AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.): Das Standard-Datenschutzmodell (V 1.1), Düsseldorf 2018.
[35] Spoerr in: BeckOK DatenschutzR, 24. Ed. 1.5.2018, DS-GVO Art. 30 Rn. 8-10.
[36] Leeb/Liebhaber: Grundlagen des Datenschutzrechts, in: JuS 2018,S. 537.
[37] Albrecht/ Jotzo: Das neue Datenschutzrecht der EU, 1. Aufl. 2017, S. 52.
[38] Frenzel in: Paal/Pauly Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 Rn. 34.

3.2.2 Transparenz

Auch die Transparenz ist ein ausdrücklich in Art. 5 Abs. 1 lit. a) DSGVO niedergeschriebenes Grundprinzip der Verarbeitung personenbezogener Daten, dass wie die Datenminimierung bei der Planung der Datenverarbeitung (Art. 25 DSGVO) zu berücksichtigen ist. Die geplanten Schritte zur Herstellung der Transparenz gemäß Art. 14, 15, 19 und 34 DSGVO sind dann wiederum durch geeignete technische und organisatorische Maßnahmen nach Art. 30 und 32 DSGVO abzusichern. Die Transparenzanforderungen sollen neben den Betroffenen auch Kontrollinstanzen (über Art. 30 und 33 DSGVO) und den Verantwortlichen selbst (Art. 30 DSGVO) in die Lage versetzen Verarbeitungsvorgänge jederzeit nachvollziehen zu können.

Dieser Retrospektive steht die Vorhersagbarkeit der Datenverarbeitung gegenüber, die ebenso der Transparenzanforderung zuzuordnen ist.[39] Dem Verantwortlichen werden aus diesem Grund verschiedene Informationspflichten auferlegt (Art. 7 Abs. 2 und 13 DSGVO). Diese Anforderung gegenüber dem Betroffenen wird in der Regel durch eine Datenschutzerklärung, die Vertragsbedingungen, sowie Aus- bzw. Abwahlmöglichkeiten (Opt-in vs. Pflichtfelder) erfüllt. Hierbei geht es darum, dass der Betroffene mögliche Auswirkungen der Datenverarbeitung abschätzen kann **bevor** überhaupt eine Datenverarbeitung stattfindet.

Die Anbieter von Identitätsschutzmodellen sollten daher in der Lage sein die notwendigen Informationen, die Art und Weise der Verarbeitung betreffend, zur Verfügung zu stellen und den Betroffenen hinreichend über die Datenverarbeitungsvorgänge aufzuklären. Hierzu zählen unter anderem Angaben zur Herkunft der Daten, den Zwecken der Verarbeitung, der Rechtsgrundlage, den Datenkategorien, zu Empfängern innerhalb und außerhalb der EU, zum Verantwortlichen und Datenschutzbeauftragten, zur Speicherdauer sowie zu Betroffenenrechten (Art. 13, 14 und 15 DSGVO). Im Rahmen der Informationspflichten sind auch weitere Verarbeitungstätigkeiten zu benennen, insbesondere wenn diese mit dem ursprünglichen Zweck der Verarbeitung nicht mehr vereinbar sind (Zweckänderung nach Art. 6 Abs. 4 DSGVO).[40]

3.2.3 Verfügbarkeit

Als einer der drei Hauptaspekte der Datensicherheit stellen die Anforderungen an die Verfügbarkeit auf Seiten des Verantwortlichen zunächst sicher, dass dieser Daten wie geplant verarbeiten kann. Gemäß Art. 32 DSGVO zählen hierzu Präventions- und Wiederherstellungsmechanismen, die ein dem Risiko angemessenes Schutzniveau erzeugen.[41] Hier sind zwei Perspektiven einzunehmen.

---

[39] Frenzel in: Paal/Pauly, Art. 5 Rn. 21.
[40] Albrecht/ Jotzo: Das neue Datenschutzrecht der EU, 1. Aufl. 2017, S. 76 f.
[41] Vgl. Gonscherowski, Hansen, Rost: Resilienz – Eine neue Anforderung aus der Datenschutz-Grundverordnung, in: DuD, 7/2018, S. 442.

Eines der entscheidenden Kriterien der Verfügbarkeit im Sinne des Datenschutzes ist, dass Berechtigte tatsächlich Zugriff auf die Daten haben. Berechtigte sind sowohl der Betroffene wie auch die (rechtmäßig) verarbeitende Stelle. Unter den Gesichtspunkten eines Identitätsschutzes sollte Letztere festlegen, nach welchen Daten gesucht werden soll und wo nach diesen gesucht werden kann. Sie ist aber auch dafür verantwortlich, dass einerseits unberechtigte keinen Zugriff auf die eigenen Datenbestände erlangen, andererseits Berechtigten der Zugriff nicht durch Unberechtigte entzogen werden kann, beispielsweise durch einschleusen eines Erpressungstrojaners. Die zweite Perspektive sollte sein, wie die Erkenntnisse über einen Identitätsdiebstahl dem Betroffenen zugänglich gemacht werden. Dies Betrifft sowohl die konkrete Zugriffsmöglichkeit, wie auch den notwendigen Informationsgehalt, beispielsweise Art und Gestaltung bzw. Formulierung einer Mitteilung. Darüber hinaus hat der Betroffene gemäß Art. 20 Abs. 2 DSGVO unter Umständen auch das Recht die gewonnenen Erkenntnisse von einem Anbieter zu einem anderen übertragen zu lassen.

Der Betroffene sollte über entsprechende für ihn/sie praktikable Zugriffswege auf die Funde verfügen. Die Auffindbarkeit der Daten kann auf verschiedene Art und Weise sichergestellt werden, muss für den Betroffenen jedoch nachvollziehbar sowie konkret anwendbar sein. Eine Zeilennummer in einer Tabelle für einen Datensatz würde diese Anforderung beispielsweise nicht erfüllen, da der Betroffene diese nicht kennt. Für die technische Auffindbarkeit des Systems reicht diese Information ggf. schon aus.

3.2.4 Integrität

Integritätsanforderungen sind ebenfalls auf verschiedenen Ebenen zu erfüllen. Die technische Seite des Grundprinzips Integrität (Art. 5 Abs. 1 lit. f) DSGVO) bezieht sich - wie die Verfügbarkeit – auf Maßnahmen zur Gewährleistung der Datensicherheit. Entsprechend sind die Anforderungen der Artikel 25 und 32 DSGVO zu erfüllen. Das datenverarbeitende System soll hierbei innerhalb der festgelegten Parameter arbeiten und Maßnahmen der IT-Sicherheit sollen vor Verlust, Zerstörung oder Schädigung schützen.[42]

Die inhaltliche Ebene wird durch Art. 5 Abs. 1 lit. d) DSGVO erfasst. Der Betroffene soll sich darauf verlassen können, dass die Informationen, die vom System verarbeitet werden, sich auch tatsächlich auf ihn/sie beziehen. Integrität im Sinne der Richtigkeit fordert die Aktualisierung, Berichtigung und die Löschung unrichtiger Daten ein. Die Aktualisierungspflicht besteht nicht durchgehend, sondern ist von einer Notwendigkeit abhängig. Einerseits soll so sichergestellt werden, dass Entscheidungen aufgrund veralteter Daten nicht zum Risiko für den Betroffenen werden. Andererseits spiegelt sich hier die Erforderlichkeit und damit Verhältnismäßigkeit im weiteren Sinne wieder.[43] Denn eine ständige oder gar lückenlose

[42] AK Technik: SDM, S. 13.
[43] Frenzel in: Paal/Pauly, Art. 5 Rn. 40.

Aktualisierung der Daten ohne hinreichenden Grund widerspricht dem Grundsatz der Datenminimierung.

Ein Identitätsdiebstahl führt häufig zu einer Beeinträchtigung der Integrität in anderen Verarbeitungskontexten, da Handlungen des Identitätsdiebes sich negativ auf dort vorhandenen personenbezogenen Daten des Opfers auswirken können. Die Integrität der Daten in einem spezifischen Kontext kann damit nicht mehr gewährleistet werden.[44] Identitätsschutzmodelle sollten hier unterstützend auf die Berichtigung oder Löschung falscher Datenbestände wirken. In Bezug auf die Warndienste sollte außerdem gewährleistet sein, dass die erhobenen Daten sich tatsächlich auf den Betroffenen beziehen. Insbesondere Namen sind für sich genommen keine eindeutig identifizierenden Merkmale.[45] Es sollen also keine Fehlalarme aufgrund von Verwechslungen ausgelöst werden. Ein Identitätsschutz-Modell sollte jedoch auch keine Warnungen „verschweigen". Entsprechend sollte eine Gegenprobe oder mindestens ein weiterer Identifikator einbezogen werden können um die Integrität der Daten sicherzustellen. Eine besondere Herausforderung wird darin bestehen die Integrität zu wahren, ohne dass durch Verkettung ein umfassendes Profil gebildet wird oder zusätzliche Daten erhoben werden müssen.[46]

3.2.5 Vertraulichkeit

Die DSGVO hebt die Vertraulichkeit in Art. 5 Abs. 1 lit. f) besonders hervor. Die in der IT-Sicherheit entwickelten Standards[47] zur Herstellung und Gewährleistung von Vertraulichkeit in informationstechnischen Systemen, lassen sich in der Regel auch anwenden um die Anforderungen an Vertraulichkeit bei der Verarbeitung personenbezogener Daten gemäß Art. 25 und 32 DSGVO sicherzustellen.

Die Vertraulichkeitsanforderung scheint im Kontext unrechtmäßig im Internet veröffentlichter Daten unerfüllbar zu sein. Sie bezieht sich jedoch nicht nur auf Außenverhältnisse (externe Hacker) sondern auch auf Akteure im Innenverhältnis der Organisation, die das Identitätsschutzverfahren betreibt. Vertraulichkeit soll grundsätzlich gegenüber allen Unberechtigten gewährleistet werden und über den gesamten Lebenszyklus eines Datums von der Erhebung bis zur Löschung gewahrt bleiben. Dies schließt auch Auftragsverarbeiter (Art. 28 Abs. 3 lit. b) DSGVO) und andere der Weisung des Verantwortlichen Unterliegende mit ein (Art. 29 DSGVO).

---

[44] Frenzel in: Paal/Pauly, Art. 5 Rn. 41.
[45] Siehe Bruegger, B.: Datenschutzrelevante Merkmale digitaler Identitäten (D 2.4), März 2018, S. 17; Vgl. auch Focus Online: So häufig gibt es ihren Familiennamen weltweit, über: https://www.focus.de/wissen/mensch/namensforschung/namensforschung-so-haeufig-gibt-es-ihren-familiennamen-weltweit_id_6213679.html (abgerufen am 14.08.2018).
[46] Vgl. EU (VO) 2016/679 Erwägungsgrund 64.
[47] Vgl. BSI Grundschutz, über: www.bsi.bund.de .

3.2.6 Nichtverkettung

Personenbezogene Daten, die für einen Identitätsdiebstahl missbraucht werden können, beinhalten ein großes Schadenspotential. Einerseits stellt der Identitätsdiebstahl an sich eine Form der Verkettung dar, die nicht gewollt ist. Andererseits könnten auch die Anbieter oder Dritte im Rahmen von Marketingstrategien oder Wirtschaftlichkeitsüberlegungen ein Interesse an Daten von Opfern eines Identitätsdiebstahls zeigen. Identitätsschutzmodelle sollten dementsprechend Vorkehrungen auf technischer und organisatorischer Ebene treffen um der Gefahr einer Zweckdehnung entgegenzuwirken.

Das Verkettungspotential verschiedener Leaks muss ebenso beachtet werden. Hier ist vor allem abzuklären, ob eine Warnung mehrere Leaks kombinieren darf und wie lange die zum Zweck des Schutzes vorgehaltenen Leak-Daten gespeichert werden dürfen. Auf Grund der Zugänglichkeit des Leaks im Internet kann es passieren, dass neue Kombinationen bereits bekannter Veröffentlichungen auftauchen. Hier ist abzuwägen, ob zu Gunsten der Nichtverkettung eine erneute Warnung in Kauf genommen werden sollte.

3.2.7 Intervenierbarkeit

Intervenierbarkeit bedeutet, dass Betroffenenrechte nicht nur pro forma zu gewähren sind, sondern durch den Verantwortlichen auch tatsächlich erfüllt werden können. Ein Löschanspruch sollte demnach tatsächlich dazu führen, dass auf Verlangen des Betroffenen dessen Daten tatsächlich entfernt werden. Ebenso ist dem Widerspruch des Betroffenen oder der Rücknahme einer Einwilligung nicht nur Folge zu leisten sondern es sind auch die Voraussetzungen für die Geltendmachung dieser Rechte, z.B. durch entsprechende Schnittstellen, zu schaffen. Einschränkungen der Betroffenenrechte sind nur im Rahmen der gesetzlich vorgegebenen Grenzen möglich.

3.2.8 Konzepte

Es sollen exemplarisch Konzepte aus verschiedenen Bereichen herausgegriffen werden um verschiedene Ansätze gegen Identitätsdiebstahl und dessen Folgen im Internet zu beurteilen. Mittlerweile bieten sowohl Versicherungsgesellschaften, Auskunfteien und Dienstleistungsunternehmen sowie Forschungsinstitute, staatliche Stellen und Open Source-Projekte dem besorgten Nutzer ihre Dienste bzw. Produkte an. Aus jedem dieser Bereiche soll ein Konzept auf seine Datenschutzfreundlichkeit untersucht werden. Folgende Angebote wurden als Beispiel herangezogen:

- DEVK IdentitätsschutzPlus (Versicherung)
- meineSCHUFA Plus (Auskunftei)
- Owldetect (Dienstleister für Privat- und Geschäftskunden, z.B. Banken)
- HPI-Leak-Checker (Forschungsinstitut)
- BSI-Sicherheitstest (Staatliche Stelle)

- haveibeenpwned (Projekt)

Betrachtet werden zwei Schwerpunkte: a) Schutzmaßnahmen zur Verhinderung eines Identitätsdiebstahls und b) Gegenmaßnahmen nach einem Identitätsdiebstahl. Alle, in den Konzepten enthaltenen, Maßnahmen werden auf ihre Datenschutzkonformität hin geprüft. Die Basis hierfür bilden die öffentlich zur Verfügung gestellten Informationsmaterialien der einzelnen Anbieter.

Ziel des Vergleichs ist es für das EIDI-Werkzeug sinnvolle Maßnahmen aufzugreifen sowie Unzulänglichkeiten bestehender Systeme nicht in EIDI zu wiederholen, um am Ende ein möglichst datenschutzfreundliches und dennoch effektives Werkzeug zu entwickeln, dass grundsätzlich mit markreifen Konzepten konkurrieren kann.

3.3 Schutz vor Identitätsdiebstahl

Der Schutz der verschiedenen Teilidentitäten einer Person ist sehr unterschiedlich ausgeprägt. Teilweise können Faktoren selbst gewählt und damit beeinflusst werden, vielfach haben Nutzer jedoch nur begrenzten oder gar keinen Einfluss auf die Schutzmaßnahmen.

3.3.1 Generische Schutzmaßnahmen

Die Maßnahmen zum Schutz vor Identitätsbetrug entsprechen im Wesentlichen denen zum verantwortungsvollen Umgang mit digitalen Angeboten im Allgemeinen. Oberstes Gebot ist Datensparsamkeit. Hierbei sollte die erste Überlegung sein, ob die Nutzung eines Angebots überhaupt notwendig ist und welcher Anbieter den jeweiligen Dienst zur Verfügung stellt.[48] Möchte der Nutzer auf ein Angebot nicht verzichten, sollten im nächsten Schritt verschiedene Dienste verglichen werden, um einen Überblick über die Datenverarbeitung sowie die Nutzungsbedingungen zu bekommen.

Nutzer sollten zudem immer reflektieren, welche Eingaben zur Nutzung eines Dienstes tatsächlich erforderlich sind, insbesondere wenn bestimmte Angaben als Pflichtfelder gekennzeichnet sind.[49] So bestehen soziale Netzwerke in ihren AGB immer noch auf die Angabe des Klarnamens obwohl es hierfür keinen zwingenden Grund gibt.[50] [51] Auch die Voreinstellungen sollten immer geprüft und ggf. datenschutzfreundlich verändert werden.

[48] ULD: Illegaler Datenhandel, über: https://www.datenschutzzentrum.de/uploads/blauereihe/blauereihe-kontodatenhandel.pdf (abgerufen am 11.07.2018), S. 14.
[49] ULD: Illegaler Datenhandel, S. 13.
[50] Facebook: Nutzungsbedingungen – Deine Verpflichtungen gegenüber Facebook und unserer Gemeinschaft, über: https://de-de.facebook.com/legal/terms/update (abgerufen am 11.07.2018).
[51] Xing: AGB – Allgemeine Pflichten des Nutzers und besondere Bestimmungen des sozialen Netzwerks, über: https://www.xing.com/terms#a-4 (abgerufen am 11.07.2018).

Eine weitere Maßnahme besteht darin digitale Identitäten voneinander zu getrennt zu halten. Dies beginnt bereits beim Anlegen von Nutzerkonten. Die Vielzahl digitaler Identitäten, die heute von einem einzigen Individuum genutzt werden können, sollte durch sichere Login-Credentials gegen Fremdzugriffe gesichert werden. Im Idealfall verwendet der Nutzer daher für jede digitale Identität einen eigenen Nutzernamen und ein eigenes Passwort.

Das Passwort sollte den aktuellen Anforderungen an ein sicheres Passwort genügen, also lang und hinreichend komplex sein. Um die Sicherheit für den Login noch zu erhöhen, kann auch auf eine 2-Faktor-Authetifizierung zurückgegriffen werden. Präventiv könnten Zugangsdaten auch ohne konkreten Anlass in regelmäßigen Abständen geändert werden.[52] Das BSI empfiehlt Nutzern dies jährlich für die wichtigsten Konten zu tun. Sollte sich herausstellen, dass Zugangsdaten durch Unbefugte zur Kenntnis genommen oder geleakt wurden, wird hierdurch die Eintrittswahrscheinlichkeit eines Schadens begrenzt. Wenn ein Passwort gewechselt wird, sollten Nutzer auf jeden Fall davon absehen, schon einmal verwendete Passwörter zu recyceln und für einen anderen Dienst zu nutzen.

Darüber hinaus spielt auch die genutzte Infrastruktur und die Hard- und Software eine große Rolle. Ungeschützte Netzwerke, die Nutzung fremder Hardware oder veralteter Software sowie Konfigurationen, die allzu leicht Zugriffsmöglichkeiten einräumen, stellen immer ein Risiko für die Datensicherheit dar und erleichtern das Abfangen von Daten. Entsprechend sind die Nutzung von Verschlüsselung, das Kappen nicht benötigter Verbindungen, die Beschränkung von Rechten und regelmäßige Updates ebenfalls Teil der Präventionsmaßnahmen gegen Identitätsbetrug.

Die genannten Maßnahmen setzen beim Nutzer einerseits eine gewisse Medienkompetenz bzw. technisches Grundverständnis voraus, andererseits verlangen sie den Nutzern ein gewisses Maß an Eigeninitiative – mit entsprechendem Zeitaufwand – und Selbstdisziplin ab. Diese Voraussetzungen erfüllen die wenigsten Nutzer. Die Folge ist, dass Identitätsbetrug nicht nur weiterhin ein erstzunehmendes Risiko darstellt sondern dass Nutzer sich diesem Risiko hilflos ausgeliefert fühlen. Dies führt schließlich zu einer Abstumpfung gegenüber Warnhinweisen und Breach-Meldungen.

Maßnahmen nach einem Identitätsdiebstahl

Je nachdem, welche Daten missbräuchlich verwendet werden, wird die Heilung eines Identitätsbetruges mehr oder weniger aufwändig sein. Der Aufwand bestimmt sich danach, wie stabil die jeweilige Teilidentität ist. Theoretisch ist die wirksamste Gegenmaßnahme gegen einen Identitätsbetrug, die betroffene Teilidentität auszulöschen, damit kein weiterer Schaden entstehen kann. Für den Betroffenen stellt sich jedoch dann die Frage der Verhältnismäßig-

[52] BSI: Mit sicheren Passwörtern private Daten Schützen, über: https://www.bsi-fuer-buer-ger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Passwoerter.html;jsessionid=BDEA2EDBFEBD7993E54F617290BBED21.2_cid369 (abgerufen am 13.09.2018).

keit zwischen dieser drastischen Maßnahme und möglichen Risiken bzw. Schäden für den Betroffenen oder Dritte.

Bei einem gehackten Profil in einem sozialen Netzwerk kann die Löschung/Sperrung des Profils durch den Dienstbetreiber oder angestoßen durch andere Nutzer erfolgen. Die Notwendigkeit für diesen Schritt ergibt sich möglicherweise dadurch, dass der Identitätsbetrüger andere Nutzer angegriffen, beleidigt oder verleumdet hat und der damit verursachte Vertrauens- und Reputationsverlust für den Identitätsinhaber nicht rückgängig gemacht werden kann. Der mit der Löschung des Profils zusammenhängende Datenverlust stellt jedoch auch einen Schaden für den Betroffenen dar.

Identitätsdiebstahl kann im Kontext dieses Dokuments daher als Kombination aus einer unrechtmäßigen Verwendung personenbezogener Daten und einer weiteren rechtlich sanktionierten Tat verstanden werden.[53]

3.3.2 Versicherungen

Das Beispiel unten stellt eine Variante einer Identitätsschutzversicherung dar, wie sie in Deutschland angeboten wird. Die Beschreibung des Sachverhalts stellt den zum Zeitpunkt der Recherche aktuellen Stand der verwendeten Dokumente dar und beruht auf im Internet frei verfügbaren Informationen auf den Webseiten des Anbieters.

Sachverhalt

Das Beispiel „Identitätsschutz Plus“ der DEVK soll die Daten des Versicherten durch einen „Online-Monitor“ und einen „Online-Cleaner“ schützen, bietet eine Notfall-Beratung und enthält außerdem eine allgemeine Rechtsberatung und eine spezielle Beratung bei privaten Urheberrechtsverstößen.[54] Auf letzteres wird an dieser Stelle nicht weiter eingegangen. Die Versicherung beauftragt einen Dienstleister – Affinion International GmbH - mit der Suche nach Kundendaten via Online-Monitor und der Online-Cleaner. Im Portfolio von Affinion heißt das Produkt IDPROTECT.

Bis zu 12 Kategorien kann der Versicherte mit seinen Daten befüllen. Nach diesen wird dann täglich das Internet (Surface Web) sowie das Deep/Dark Web durchsucht. Innerhalb der der Kategorien E-Mail-Adresse und Mobilfunknummer können zudem 5 bzw. 3 Einzel-

[53] Vgl. Koops/ Leenes: Identity Theft, Identity Fraud and/or Identity-related Crime, in DuD 9/2006, S. 554.
[54] DEVK Identitäts-Schutz PLUS: Leistungen im Überblick, über: https://www.devk.de/produkte/rechtsschutz/identitaetsschutzplus/index.jsp (abgerufen am 03.07.2018).

angaben eingetragen werden.[55] Findet sich ein Treffer wird der Betroffene wahlweise per E-Mail oder SMS benachrichtigt.[56] [57]

Abb. 3: Risiko - IDPROTECT

Der Betroffene kann sich in sein IDPROTECT-Benutzerkonto[58] einloggen und hier die Suchergebnisse sowie zusätzliche Informationen einsehen. Welches Risiko der Fund aus Sicht von IDPROTECT darstellt, wird mit Hilfe einer dreistufigen Risikografik (Abb. 3) [59] angezeigt.

Hält der Betroffene eine Veröffentlichung im „Surface Web" für unberechtigt, kann die Funktion des Online-Cleaners verwendet werden.[60] Über diesen wird durch das Service-Team Kontakt zur verantwortlichen Stelle aufgenommen und die Löschung bzw. Sperrung der Daten im Namen des Betroffenen veranlasst.[61] Ist diese erfolgt, erhält der Betroffene hierüber eine Mitteilung sowie eine Kopie des im entsprechenden Fall mit der verantwortlichen Stelle geführten Schriftwechsels. Kommt der Verantwortliche der Lösch- bzw. Sperraufforderung nicht nach, erfolgt nach Ablauf einer nicht näher genannten Frist eine Erinnerung und ggf. eine erneute Kontaktaufnahme.

Diese Möglichkeit besteht für Funde im Deep/Dark Web nicht, denn: *„Aufgrund der Struktur und der Anonymität im Deep & Dark Web kann der Online-Cleaner für Treffer in diesen Bereichen nicht angeboten werden."*[62]

Auch für Funde im Surface Web gibt es Einschränkungen in Bezug auf die Sperrung bzw. Löschung von Einträgen, z.B. wenn kein Anspruch auf Löschung oder Sperrung besteht oder der Kunde für das jeweilige Meldesystem der verantwortlichen Stelle benötigte, zusätzliche Informationen nicht zur Verfügung stellt bzw. wenn der Betroffene die Löschung nur selbst veranlassen kann.[63]

---

[55] IDPROTECT FAQ's: Wie werde ich von IDPROTECT über Treffer benachrichtigt?, über: https://www.idprotect.de/Content.aspx?content=faq (abgerufen am 17.07.2018).
[56] IDPROTECT Online-Monitor: Surface Web Suche, über: https://www.idprotect.de/Content.aspx?content=surfaceweb (abgerufen am 03.07.2018).
[57] IDPROTECT Online-Monitor: Deep und Dark Web Suche, über: https://www.idprotect.de/Content.aspx?content=darkweb (abgerufen am 03.07.2018).
[58] Startseite von IDPROTECT von Affinion GmbH, über: https://www.idprotect.de/Default.aspx?source=XYvld8floRDfkYCa7jmu9Q%3d%3d (abgerufen am 03.07.2018).
[59] Affinion GmbH: IDPROTECT, über: https://www.idprotect.de/Default.aspx (abgerufen am 10.07.2018).
[60] IDPROTECT Online-Monitor: Surface Web Suche, über: https://www.idprotect.de/Content.aspx?content=surfaceweb (abgerufen am 03.07.2018).
[61] IDPROTECT Online-Cleaner, über: https://www.idprotect.de/Content.aspx?content=onlinecleaner (abgerufen am 03.07.2018).
[62] IDPROTECT Online-Cleaner.
[63] IDPROTECT Online-Cleaner.

Für den Fall das Daten eines Kunden im Deep/Dark Web gefunden werden, kann dieser sich mit dem Service-Team in Verbindung setzen oder Handlungsempfehlungen im Hilfebereich des Nutzerkontos nachlesen.[64]

Allgemeine Geschäftsbedingungen der DEVK (AGB-DEVK)

Grundlage der Datenverarbeitung ist ein Vertrag. Die DEVK schließt mit dem Kunden einen Vertrag über eine Rechtschutzversicherung ab. Der Identitäts-Schutz PLUS gehört zu den Premiumleistungen verschiedener Rechtsschutzversicherungstarife.[65]

Der Versicherungsschutz schließt neben dem Hauptversicherten z. T. auch Lebenspartner und im Haushalt lebende Familienangehörige mit ein.[66] Die DEVK stellt die zur Erstellung des Nutzerkontos erforderlichen Daten (Versicherungsnummer und DEVK-Passwort) in einem Begrüßungsschreiben (per Post) zur Verfügung.[67] Die eigentliche Versicherungsleistung „Identitäts-Schutz im Internet und Dark/Deep Web" (IDPROTECT) wird von Affinion GmbH erbracht. Eine Verpflichtung zur Nutzung des Produkts besteht nicht:

„Wir sorgen dafür, dass Sie auf Wunsch durch ein entsprechendes Dienstleistungsunternehmen ein tägliches ***Monitoring*** *Ihrer persönlichen Identitätsdaten im Internet[…] durchführen lassen können…"*[68]*. (Unterstreichung durch die Autorin, Hervorhebung im Text)*

Dienstleister in Bezug auf die Datenverarbeitung sind laut Code of Conduct (CoC) der Versicherungswirtschaft Unternehmen oder Personen, die eigenverantwortlich Aufgaben für das Unternehmen (DEVK) wahrnehmen.[69] In diesem Fall die Affinion GmbH.

Allgemeine Geschäftsbedingungen Affinion GmbH (AGB-Affinion)

Die Registrierung erfolgt direkt beim Dienstleister. Die Registrierungsseite ist über die Webseite der DEVK verlinkt. Nimmt der Kunde die angebotene Dienstleistung in Anspruch und registriert ein entsprechendes Nutzerkonto für IDPROTECT, kommt damit ein gesonderter

---

[64] IDPROTECT Online-Monitor: Deep und Dark Web Suche, über: https://www.idprotect.de/Content.aspx?content=darkweb (abgerufen am 03.07.2018).
[65] DEVK: Kundeninformationen zur Rechtsschutzversicherung für Nichtselbstständige (Stand 01.05.2018), über: https://www.devk.de/media/content/download/produkte/rechtsschutz/DEVK-RS-Kundeninfo-50080-2018-05.pdf (abgerufen am 12.07.2018), S. 36 f, 46, 55, 65, 73, 82 f.
[66] Vgl. DEVK: Kundeninformationen zur Rechtsschutzversicherung für Nichtselbstständige.
[67] DEVK: Informationsblatt zum Identitätsschutz, über: https://www.devk.de/media/content/download/produkte/rechtsschutz/DEVK-RS-Infoblatt-Identitaetsschutz-50005-2017-01.pdf (abgerufen am 12.07.2018), S. 3.
[68] DEVK: Kundeninformation zur Rechtsschutzversicherung für Nichtselbstständige, S. 36.
[69] CoC der Versicherungswirtschaft, über: https://www.gdv.de/resource/blob/23938/4aa2847df2940874559e51958a0bb350/download-code-of-conduct-data.pdf (abgerufen am 13.09.2018), S. 4.

Vertrag zwischen dem Kunden und Affinion zustande. Dieser Vertrag besteht laut Affinion aus dem Willkommensschreiben, den AGB-Affinion und der Datenschutzerklärung.[70]

Nutzungsberechtigte sind gemäß Nr. 2 AGB-Affinion neben dem Hauptversicherten bis zu 3 weitere Mitversicherte, die im gleichen Haushalt leben (und mindestens 7 Jahre alt sind). Die Dienstleistung kann solange in Anspruch genommen werden, wie ein Vertragsverhältnis mit der DEVK besteht. Der Online Monitor und der Online Cleaner entsprechen dem oben beschriebenen Leistungsumfang. Ein Nutzerkonto für Mitversicherte kann nur der Hauptversicherte anlegen.

Die Datenschutzbestimmungen sind in einer separaten Datenschutzerklärung geregelt, soweit sie die Datenverarbeitung nach der Registrierung betreffen. In Nr. 8-10 AGB-Affinion werden jedoch einige Regelungen mit Datenschutzbezug explizit genannt.[71]

Neben dem Ausschluss der rechtswidrigen Nutzung des Service sowie der Vereinbarung zur Aktualität der Profildaten und der Geheimhaltung der Zugangsdaten, wird an dieser Stelle festgelegt, dass die Eingabe von Daten Dritter nicht gestattet ist.[72] In Nr. 9 wird der Hauptversicherte dazu verpflichtet die Einwilligung für die Weitergabe der E-Mail-Adresse der Mitversicherten durch Affinion einzuholen.[73] Diese Einwilligung umfasst außerdem die Erlaubnis den/die Mitversicherten via E-Mail zu kontaktieren und die benötigten Login-Informationen per E-Mail zu übersenden.[74]

Verwendet der Mitversicherte diese Login-Daten kommt zwischen diesem und Affinion ein Nutzungsvertrag zustande. Dem Hauptversicherten wird die Verantwortung der für die Einhaltung der AGB und insbesondere der darin enthaltenen „Wohlverhaltensregeln“ übertragen.[75] Ein Anspruch auf Einsicht in die Profil-Informationen der Mitversicherten durch den Hauptversicherten besteht nicht, wohl aber die Verpflichtung die Einhaltung der AGB durch die Mitversicherten zu überwachen. Der Hauptversicherte kann lediglich die Löschung eines Profils vornehmen. Im Zuge dessen werden alle darin enthaltenen Informationen gelöscht. Affinion rät daher dem Hauptversicherten diesen Schritt ggf. vorher mit dem Mitversicherten abzusprechen.

---

[70] IDPROTECT: Allgemeine Geschäftsbedingungen (Stand Mai 2018), über: https://www.idprotect.de/bca/datapal15_de_devk/Default/pdf/161118_devk_idprotect_agb_kd_Ansicht_sj.pdf (abgerufen am 12.07.2018), S. 1.
[71] IDPROTECT: Allgemeine Geschäftsbedingungen (Stand Mai 2018), S. 2-3.
[72] IDPROTECT: Allgemeine Geschäftsbedingungen (Stand Mai 2018), Nr. 8, S. 2 f.
[73] IDPROTECT: Allgemeine Geschäftsbedingungen (Stand Mai 2018), Nr. 9, S. 3.
[74] IDPROTECT: Allgemeine Geschäftsbedingungen (Stand Mai 2018), Nr. 8, S. 3.
[75] IDPROTECT: Allgemeine Geschäftsbedingungen (Stand Mai 2018), Nr. 8, S. 3.

Die öffentlich verfügbare Datenschutzerklärung deckt laut Nr. 1 auch die Datenverarbeitung der registrierungspflichtigen Dienstleistungen mit ab.[76] Sie enthält die in einer Datenschutzerklärung üblichen Angaben zu Datenkategorien, Verarbeitungsschritten, Speicherdauer und Ansprechpartnern (Verantwortliche Stelle und Datenschutzbeauftragter).

Ein Hinweis zur Datenverarbeitung im Rahmen von IDPROTECT findet sich lediglich an einer Stelle unter 4.2.: Hier wird darauf hingewiesen, dass die Nutzung des Online-Monitor-Service abhängig von der Verwendung von Cookies ist.[77]

Auf Grund von berechtigten Interessen behält Affinion sich die Nutzung personenbezogener Daten vor. Berechtigte Interessen:

„[…]umfassen die Interessen Affinions an der Leitung und Durchführung Ihrer geschäftlichen Tätigkeiten, damit es uns möglich ist, Ihnen den bestmöglichen Service und ein sicheres Erlebnis zu bieten. […] Wenn Sie widersprechen, kann es in den Fällen, in denen wir Daten aufgrund eines berechtigten Interesses erheben, Auswirkungen auf unsere Möglichkeiten haben, Aufgaben in Ihrem Interesse auszuführen."[78]

Mit einem berechtigten Interesse begründet Affinion das Speichern von Feedbackinformationen, die Gesprächsaufzeichnungen bei Kontakt mit dem Kundenservice und das Teilen bzw. die Übermittlung und Weitergabe von Daten an Unternehmensteile und Dritte zu Marketing und IT-Sicherheitszwecken.

In der Datenschutzerklärung wird ebenfalls darauf verwiesen, dass die Datenweitergabe bzw. Übermittlung innerhalb des Unternehmens weltweit und auch mit Dritten erfolgen kann.[79] Obwohl dieser Hinweis sich im Abschnitt zur Verwendung anonymisierter Daten findet, wird diese Einschränkung dahingehend wieder aufgehoben, dass diese mit personenbezogenen Daten verknüpft werden können.

Schlussfolgerungen

Das IDPROTECT- bzw. Identitäts-Schutz PLUS-Angebot der DEVK ermöglicht seinen Kunden eine automatische Warnung vor einem potentiellen Identitätsdiebstahl. Auswertungen über Anzahl und Erfolg der Warnung sind leider nicht öffentlich verfügbar. Das Schutzkonzept ermöglicht den Kunden sensible Daten, wie Bankverbindungen, wichtige Nummern und Kontaktdaten nach eigenem Ermessen überwachen zu lassen und regelmäßig informiert zu werden. Die Alarmfunktion sorgt zudem dafür, dass im Falle eines möglichen Data Breaches der Kunde frühzeitig gewarnt wird. Eine auf den ersten Blick hilfreiche Dienstleis-

[76] Affinion: Datenschutzerklärung IDPROTECT (Stand: 04. Mai 2018), über: https://www.idprotect.de/bca/datapal15/Default/pdf/20161223_IDPROTECT_Datenschutzbestimmungen.pdf (abgerufen am 13.07.2018), S. 1.
[77] Affinion: Datenschutzerklärung IDPROTECT, S. 5.
[78] Affinion: Datenschutzerklärung IDPROTECT, S. 4.
[79] Affinion: Datenschutzerklärung IDPROTECT, S. 4f.

tung scheint auch die Online-Cleaner-Funktion zu sein, die dem Nutzer den Zeitaufwand für die Entfernung unerwünschter Veröffentlichungen ersparen kann. Auch hierzu gibt es leider keine Auswertungen, in wie vielen Fällen dies tatsächlich der Fall war. Inwieweit die 24-Stunden-Telefonhilfe den Kunden – auch im Falle eines Datenschutzvorfalls – kompetent berät, kann hier nicht beurteilt werden. Da das Produkt Bestandteil einer Rechtschutzversicherung ist, erfolgt wahrscheinlich zumindest die Weiterleitung an einen Rechtsanwalt. Aus Datenschutzsicht gibt es dennoch einige Kritikpunkte.

Transparenz

Die DEVK verweist in ihren AGB darauf, dass das Monitoring von einem Dienstleistungsunternehmen erbracht wird. Dienstleister handeln laut Begriffsdefinition des CoC eigenverantwortlich (s.o.). Da ein Auftragsverarbeiter im Sinne der DSGVO weisungsgebunden wäre, kann Affinion dementsprechend nur Verantwortlicher sein.[80] Die gemeinsame Verantwortlichkeit im Sinne des Art. 26 DSGVO bestimmt sich durch gemeinsame die Entscheidung über die Zwecke und Mittel der Verarbeitung aus. Im konkreten Fall entscheidet die DEVK über die angebotene Dienstleistung (Zweck) und den Dienstleister, der mit der Erbringung des angebotenen Service betraut wird (Mittel). Die genaue Durchführung der Suche nach den Daten (Mittel) sowie die Benachrichtigung über konkrete Funde (Zweck) erfolgt dann durch den Dienstleister selbst, ist jedoch abhängig von einer bestehenden Vertragsbeziehung zwischen der Versicherung und dem Kunden. Aus diesem Umstand ergibt sich in der Datenschutzerklärung von Affinion bereits die erste Unklarheit, denn hier heißt es: „Bitte sehen Sie [in] die AGB, um zu verstehen ob wir der Datenverantwortlicher oder der Datenverarbeiter Ihrer Daten sind.“[81] Die Klärung dieser Frage liegt jedoch nicht beim Kunden und widerspricht zudem dem Transparenzgebot der Grundverordnung.

Die aus Art. 26 Abs. 1 DSGVO folgenden Verpflichtungen hinsichtlich der Verfügbarkeit wesentlicher Informationen zur Festlegung der Zusammenarbeit müssen dem Kunden zur Verfügung gestellt werden. Hierzu zählt grundsätzlich auch die Information darüber, dass eine gemeinsame Verantwortlichkeit besteht und welche Stelle welche Aufgaben und Pflichten übernimmt.[82] Sowohl im Außenverhältnis zwischen Kunden und verantwortlichen Stellen wie auch im Innenverhältnis zwischen den gemeinsam Verantwortlichen soll die Vereinbarung Rechtssicherheit herstellen.[83] [84] Da der Kunde weder die branchenüblichen Begriff-

[80] GDV: Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft (Stand 07.09.2012), Art. 22.
[81] Affinion: Datenschutzerklärung IDPROTECT, S. 1.
[82] DSK: Kurzpapier Nr. 16, über: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_16_Gemeinsame-Verantwortliche.pdf (abgerufen am 14.09.2018), S. 3-4.
[83] Vgl. Martini in Paal/Pauly: Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 26 Rn. 3-4 und 10.

lichkeiten kennt und auch keine Kenntnisse datenschutzrechtlicher Begriffsdefinitionen oder sonstige juristische Vorkenntnisse vorausgesetzt werden können, sind die Informationen in einer angemessene Form und Sprache zu gestalten (ErwG 58: „präzise, leicht zugänglich und verständlich"), um dem Transparenzgebot zu genügen. Auch wenn die DSGVO keine Vorgaben zum Format der Vereinbarung vorgibt, ist davon auszugehen, dass die Kernpunkte zumindest an ein und derselben Stelle, z.B. auf einer Webseite zur Verfügung gestellt werden müssen, da nur auf diese Weise die Anforderung des Art. 26 Abs. 2 DSGVO erfüllt werden kann.[85] [86] Zu bemängeln ist auch die grammatikalisch fehlerhafte sprachliche Umsetzung, die die Anforderung „verständlich" nicht erfüllt.

Die AGB der DEVK und der Affinion sind in Bezug auf die Nutzungsberechtigten widersprüchlich. Während die DEVK in ihren Versicherungsbedingungen die Mitversicherten nicht auf eine bestimmte Personenzahl begrenzt, lässt Affinion maximal 3 weitere Nutzungsberechtigte zu.[87] Ein weiterer Kritikpunkt bezüglich der Transparenz ist die Nutzerregistrierung Mitversicherter für IDPROTECT. Damit auch Mitversicherte den Service nutzen können, muss der Hauptversicherte ein Nutzerkonto anlegen und Affinion die E-Mail-Adresse des Versicherten mitteilen, für den das zusätzliche Konto bestimmt ist. Die Einwilligung für die Weitergabe der E-Mail-Adresse an Affinion sowie für das Senden des Begrüßungsschreibens an diese E-Mail-Adresse muss der Hauptversicherte vom Mitversicherten einholen. Dies ist in zweierlei Hinsicht unverständlich, denn erstens spricht nichts dagegen, dass der Mitversicherte das Nutzerkonto selbst anlegt und zweitens ist die Weitergabe der E-Mail-Adresse eine für den Vertragsschluss zwischen Affinion und dem Mitversicherten erforderliche vorvertragliche Datenverarbeitung, die keiner Einwilligung bedarf.[88] Es ist mit großer Wahrscheinlichkeit zu verneinen, dass die durch den Hauptversicherten eingeholte Einwilligung den Anforderungen von Art. 7 DSGVO genügt und dass Affinion den Nachweis darüber, dass eine gültige Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO vorlag, erbringen bzw. dem Hauptversicherten aufbürden kann. Jedenfalls könnten alle notwendigen Informationen auch bei der ersten Kontaktaufnahme mit dem Mitversicherten zur Verfügung gestellt werden. Art. 14 DSGVO und ErwG 61 stellen dies ausdrücklich klar.

Eine eigene Datenschutzerklärung für den Identitätsschutz gibt es weder bei der DEVK noch bei Affinion, es gilt die Datenschutzerklärung des jeweiligen Verantwortlichen. Da für die Erbringung der Dienstleistung allein der Dienstleister Affinion zuständig ist, beschränken

---

[84] Der CoC wurde zwischenzeitlich um einen Abschnitt zu gemeinsamen Verantwortlichkeit ergänzt (Art. 22 a) CoC). Dieser bezieht sich jedoch auf Versicherungs- und Finanzdienstleistungsunternehmen.
[85] DSK: Kurzpaier Nr. 16, S. 4.
[86] Breyer: Verarbeitungsgrundsätze und Rechenschaftspflicht nach Art. 5 DS-DVO, in: DuD (Vol. 42) Nr. 5/18, S. 312.
[87] Vgl. DEVK: Kundeninformation zur Rechtsschutzversicherung, S. 34, 43; Vgl. IDPROTECT: Allgemeine Geschäftsbedingungen (Stand Mai 2018), S. 1.
[88] Siehe Erwägungsgrund (EwG) 44 VO (EU) 2016/679.

sich die datenschutzrechtlichen Verpflichtungen der DEVK in Bezug auf den Identitäts-Schutz PLUS darauf, dass ggf. Daten des Kunden zwischen dieser und Affinion beispielsweise zu Abrechnungszwecken übermittelt werden. In jedem Fall werden die Daten genutzt um die erneute Anmeldung nach einer AGB-Verletzung mit anschließendem Ausschluss zu verhindern.[89]

Die Datenschutzerklärung von Affinion erfüllt nicht die Anforderungen der DSGVO.[90] Grundlegende Prinzipien nach Art. 5 DSGVO, wie Transparenz, Verarbeitung nach Treu und Glauben sowie der Zweckbindungsgrundsatz werden nicht eingehalten. Will der Kunde sich für den Service IDPROTECT registrieren, müssen für die Nutzerkontoerstellung mindestens eine E-Mail-Adresse und die Versicherungsnummer angegeben werden um den Service in Anspruch nehmen zu können. Diese Daten sind gemäß Art. 6 Abs. 1 lit. b) DSGVO zur Vertragserfüllung erforderlich.

Unklar ist hingegen, wie mit allen weiteren personenbezogenen Daten verfahren wird. Will der Kunde IDPROTECT in vollem Umfang nutzen, gibt er unter anderem (1) Namen und Kontaktinformationen sowie (2) Zahlungsinformationen an. Wie diese Daten genutzt werden, hängt laut Affinion vom genutzten Service (hier der Online-Monitor) ab, aber auch davon, ob es sich um eine bezahlte Dienstleistung oder ein Paket handelt. Welche Auswirkungen die jeweilige Variante auf die Datennutzung hat, wird jedoch nicht näher erläutert. Es ist zweifelhaft, dass eine derart unspezifische Formulierung den Bestimmtheitsgrundsatz für die Zwecke der Verarbeitung erfüllt, da für den Betroffenen nicht ersichtlich ist, wofür die Daten ggf. noch genutzt werden sollen.[91] [92]

Zu kritisieren ist auch die Passage zur Datenverarbeitung aufgrund eines berechtigten Interesses. Hier heißt es: *„Wenn Sie* [der Datenverarbeitung] *widersprechen, kann es in den Fällen, in denen wir Daten aufgrund eines berechtigten Interesses erheben, Auswirkungen auf unsere Möglichkeiten haben, Aufgaben in Ihrem Interesse auszuführen."*[93] Dies kann aber nicht möglich sein, denn die Aufgabenerfüllung ist vertraglich geregelt und alle Daten, die erforderlich zur Vertragserfüllung sind, werden eben gerade nicht aufgrund eines berechtigten Interesses verarbeitet. Es wird ein Zusammenhang konstruiert, der die Erfüllung des Vertrages und anderer Pflichten („sicheres Erlebnis") von der Durchsetzung berechtigter Interessen des Verantwortlichen abhängig macht. Dies stellt eine unzulässige Vorgehensweise dar, denn die Einhaltung ge-

[89] Affinion: Datenschutzerklärung IDPROTECT, S. 2.
[90] Die von Affinion für IDPROTECT zur Verfügung gestellte Datenschutzerklärung (Stand 04. Mai) ist auch am 09.08.2018 (also lange nach Geltungsbeginn der DSGVO am 25. 05.2018) noch unverändert abrufbar gewesen. Affinion suggeriert damit dem Kunden, dass IDPROTECT den aktuellen Anforderungen der DSGVO entspricht.
[91] Artikel-29-Datenschutzgruppe: Opinion 03/2013 on purpose limitation, WP 203, über: https://iapp.org/media/pdf/resource_center/wp203_purpose-limitation_04-2013.pdf (abgerufen am 09.08.2018), S. 16.
[92] Breyer: Verarbeitungsgrundsätze, S. 313.
[93] Affinion: Datenschutzerklärung IDPROTECT, S. 4.

setzlicher Verpflichtungen, wie beispielsweise die Gewährleistung der Sicherheit („sicheres Erlebnis“) der Verarbeitung gemäß Art. 32 DSGVO, ist unabhängig von den Voraussetzungen einer rechtmäßigen Verarbeitung zu erfüllen. Die Einhaltung der DSGVO ist somit grundsätzlich keine Rechtfertigung für ein berechtigtes Interesse.[94] Welche Interessen genau verfolgt werden, ist nicht näher beschrieben, sodass auch keine Beurteilung möglich ist, ob ggf. die Grundrechte der Betroffenen überwiegen würden.

Ein berechtigtes Interesse wird auch als Grundlage zum weltweiten Teilen von Daten innerhalb der Affinion Unternehmensgruppe angeführt: *„es kann vorkommen, dass wir Ihre Daten an mit uns verbundene Unternehmen* […] *weltweit weitergeben*…“[95]. Die Angaben sind insgesamt zu ungenau. Kategorien von Empfängern werden nicht genannt und es ist nicht eindeutig, unter welchen Umständen ein Datentransfer stattfinden und ob eine Übermittlung in Drittstaaten erfolgt.

In Zusammenhang mit den im oben genannten Absatz aufgeführten Angaben, drängt sich die Frage auf, wie und aus welchen Quellen Affinion eigentlich die Informationen zu den im Online-Monitor eingegebenen Daten erhält. Die Quellen sind in den öffentlich verfügbaren Informationen nicht näher beschrieben. Affinion gibt lediglich an, neben dem frei zugänglichen Internet auch das Deep und Dark Web zu durchsuchen. Wie das gemacht wird und wer die Partner sind, wird nicht erläutert.

Verkettung

Der Absatz 3.1 zur Übermittlung der Daten an Partner und ausgewählte Dritte nennt ausdrücklich Betrugsprävention durch Finanzdienstleister als Zweck für die Datenweitergabe sowie die Weitergabe an jeden anderen im Zusammenhang mit dem Service stehenden Partner. Dies lässt vermuten, dass Affinion anhand der personenbezogenen Daten des Kunden Informationen bei den entsprechenden Anbietern einholt und diese zusammenführt, auswertet und bei einem entsprechenden Verdacht eine Warnung an den Kunden ausgibt. Das würde auch erklären, wie Affinion an Informationen aus dem Deep Web gelangt. Das Deep Web besteht aus nicht öffentlich zugänglichen Datenbanken und anderen zugriffsgeschützten Inhalten unterschiedlichster Art. Dieser Teil des Internets ist über gängige Suchmaschinen nicht erreichbar, da die Seiten nicht indexiert werden können oder sollen. In dieser Konstellation bestehen für Affinion umfangreiche Möglichkeiten der Verkettung. Die Zusammenstellung für den Kunden führt automatisch dazu, dass, je mehr personenbezogene Daten für den Online-Monitor bereitgestellt werden, ein umso lückenloseres Profil desselben angefertigt wird.

[94] S. Robrahn/ Bremert: Interessenskonflikte im Datenschutzrecht, in: ZD 7/2018, S. 295.
[95] Affinion: Datenschutzerklärung IDPROTECT, S. 4.

Dieses Profil wird möglicherweise noch durch die Kombination anonymisierter bzw. aggregierter Daten vervollständigt. Die Verknüpfung anonymisierter/aggregierter Daten mit personenbezogenen Daten wird wie folgt begründet:

„Wir können Ihre Daten auch nutzen um uns eine Meinung darüber zu bilden, was Sie möglicherweise benötigen bzw. was von Interesse für Sie sein kann. Auf diese Weise können wir feststellen welche Produkte, Dienstleistungen oder Angebote von Relevanz für Sie sind."[96]

Diese Meinungsbildung steht in direktem Zusammenhang mit dem Hauptgeschäftsfeld der Affinion International GmbH. Auf der Homepage heißt es hierzu: *„Wir entwickeln, implementieren und managen Kundenbindungsprogramme für die weltweit größten Banken, Versicherungen und Telekommunikationsunternehmen. Es ist bewiesen, dass unsere Programme den Kundenwert nachhaltig erhöhen."*[97] Das Hauptgeschäftsfeld ist die Erstellung von Marketing Strategien für ihre Kunden, darunter beispielsweise Mobilcom Debitel, Royal Bank of Scottland und Telefonica.[98] Angeboten werden für Unternehmen kostengünstige Zusatzprodukte, die dem Kunden als (z.T. kostenlose) Zusatzleistung verkauft werden. Dies legt die Vermutung nahe, dass die Wertschöpfung des IDPROTECT-Produkts nicht direkt über einen Anteil am Versicherungsbeitrag erfolgt, sondern vielmehr darin besteht, dass die so gewonnenen Erkenntnisse in das Produktdesign einfließen und letztendlich Banken, Versicherungen und Telekommunikationsunternehmen diese maßgeschneiderten Dienstleistungen einkaufen und an ihre Kunden weiterverkaufen. Hier schließt sich der Kreis zur Datenverarbeitung auf Grund berechtigter Interessen von Affinion. Es handelt sich hier eben gerade nicht um ein Unternehmen aus der IT-Sicherheits- oder Datenschutzbranche, sondern um eines aus dem Marketingbereich.

Das verwendete Werkzeug zur Datenverarbeitung wird nicht nur von der DEVK, sondern auch von anderen Unternehmen Kunden als Service angeboten. Es wird an keiner Stelle in der Datenschutzerklärung oder in den AGB darauf eingegangen, wie personenbezogene Daten verarbeitet werden, die als „Beifang" durch den Online-Monitor-Service mit erhoben werden. Hier ist jedoch die Zulässigkeit der Zweckänderung der Datenverarbeitung zu prüfen, insbesondere vor dem Hintergrund der Warnfunktion als ursprünglichem Zweck.

Verfügbarkeit

Der Hauptversicherte hat die Möglichkeit Nutzerkonten für andere Mitversicherte anzulegen. Mitversicherte sind in Bezug auf Informationen zu möglichen Datenschutzvorfällen jedoch auf das Wohlwollen des Hauptversicherten angewiesen, da dieser einerseits als Einziger zusätzliche Konten anlegen kann. Andererseits kann der Hauptversicherte alle Konten jederzeit löschen, ohne dass der Betroffene hierüber in Kenntnis gesetzt wird. Mag das Anlegen eines solchen zusätzlichen Nutzerkontos noch im Ermessen des Hauptversicherten lie-

[96] Affinion: Datenschutzerklärung IDPROTECT, S. 3.
[97] https://affinion.de/ (abgerufen am 19.07.18).
[98] https://affinion.de/unsere-partner/ (abgerufen am 11.10.18).

gen, so kommt bei der ersten Anmeldung durch den Mitversicherten zwischen diesem und Affinion ein eigener Nutzungsvertrag zustande. Warum der Hauptversicherte ab diesem Zeitpunkt ein Nutzerkonto weiterhin löschen können soll, ist datenschutzrechtlich nicht nachvollziehbar. Der Betroffene müsste zumindest mit einer ausreichenden Frist vorgewarnt werden, dass die Informationen demnächst nicht mehr zur Verfügung stehen.

Eine Ausnahme wäre, dass aufgrund von Nr. 9 der AGB, wonach der Hauptversicherte die Einhaltung der AGB durch den Mitversicherten überwachen soll, bei einem Verstoß die Nutzung nur durch Löschung des Kontos unterbunden werden kann. Die Überwachung der Einhaltung der AGB ist dem Hauptversicherten jedoch kaum möglich, da die Login-Daten von Affinion an die E-Mail-Adresse des Mitversicherten gesendet wurden. Ein Zugriffsrecht durch den Hauptversicherten geht aus den vorliegenden Informationen nicht hervor. Sollte der Hauptversicherte entgegen dieser Vermutung doch Zugriffsrechte auf die Nutzerkonten der Mitversicherten haben, wäre dies eine Verletzung des Vertraulichkeitsgrundsatzes aus Art. 5 Abs. 1 lit. f) DSGVO.

Eine Löschung des Nutzerkontos hat laut AGB die Löschung aller darin enthaltenen Daten zur Folge. Die Verfügbarkeit kann somit von einem Moment auf den anderen nicht mehr gewährleistet werden. Affinion kann das Recht des Betroffenen auf Datenübertragbarkeit gemäß Art. 20 DSGVO auf diese Weise jedoch nicht mehr gewährleisten. Außerdem kann die Beweissicherung durch den Betroffenen für zivilrechtliche Ansprüche nach einem Datenschutzvorfall dadurch erheblich beeinträchtigt werden.

Vertraulichkeit

Kritikwürdig am vorliegenden Identitätsschutzmodell sind insbesondere die Maßnahmen zum Schutz der Vertraulichkeit der personenbezogenen Daten. Da der Hauptversicherte zusätzliche Nutzerkonten, beispielsweise für Familienangehörige, anlegen kann, besteht die Möglichkeit neben den eigenen auch sensible Informationen der Mitversicherten zu überwachen. Die E-Mail-Adresse, die für die Übertragung der Login-Daten verwendet wird, wird nicht weiter verifiziert, d.h. Affinion überprüft nicht, wer Zugriff auf das E-Mail-Postfach hat. Hinzu kommt, dass die Login-Daten für die zusätzlichen Nutzerkonten per E-Mail, d.h. höchstwahrscheinlich unverschlüsselt übermittelt werden.

Mit den, an die E-Mail-Adresse übersendeten, Zugangsdaten kann sich derjenige (Hauptversicherte), der Zugriff auf das E-Mail-Konto hat, dann im Nutzerkonto anmelden und die Suchparameter eingeben. Tauchen beispielsweise E-Mail-Adresse(n), Name, Kreditkarten- oder Mobilfunknummer(n) im Internet auf, würde entsprechend nicht der Betroffene sondern der Hauptversicherte informiert werden. Da bei einem Treffer im Surface Web auch

der Fundort angegeben wird, kann so direkt nachvollzogen werden, welchen Seiten und Dienste die andere Person nutzt.[99]

Dieses Risiko beschränkt sich nicht nur auf die Familienangehörigen bzw. Mitversicherten[100] sondern besteht auch für Dritte, denn die Eingabe personenbezogener Daten Dritter wird zwar in den AGB untersagt, inwiefern Affinion die Einhaltung der Vorgabe überprüft ist jedoch unklar. Aufgrund der vorliegenden Informationen muss davon ausgegangen werden, dass die Klausel in den AGB die einzige implementierte Schutzmaßnahme darstellt.

Integrität

Die Integrität der vom Online-Monitor erhobenen Daten ist grundsätzlich von der Richtigkeit der Angaben des Nutzers abhängig. Entsprechend wird dieser in den AGB dazu verpflichtet korrekte Angaben zu machen und diese ggf. zu aktualisieren.

Eine Garantie für eine vollständige Suche bzw. das Auffinden aller unbefugt veröffentlichten Daten des Kunden kann nicht gegeben werden.

Intervenierbarkeit

Der Kunde kann Änderungen zu personenbezogenen Angaben selbstständig über das Nutzerkonto vornehmen. Der Dienst von Affinion kann zudem jederzeit gekündigt werden. Kündigt der Kunde die Versicherung dessen Bestandteil IDPROTECT ist, endet automatisch auch das Vertragsverhältnis mit Affinion.

Der Kunde wird in der Datenschutzerklärung auf die entsprechenden Betroffenenrechte hingewiesen. Hier finden sich auch die Kontaktinformationen zum Datenschutzbeauftragten.

Der Übergang zwischen dem Schutz vor und den Maßnahmen nach einem Identitätsdiebstahl ist beim „Identitäts-Schutz PLUS“ fließend.

3.3.3 Auskunftei

Der folgende Sachverhalt untersucht den Identitätsschutz meineSCHUFA plus. Wie im Fall der Versicherungen handelt es sich um ein konkretes Beispiel anhand dessen das entsprechende Identitätsschutzmodell auf die Erfüllung datenschutzrechtlicher Anforderungen untersucht werden soll.

99

100 Dies gilt insbesondere für vertragsähnliche Schuldverhältnisse, wie bspw. Geschäftsführung ohne Auftrag, die aufgrund der fehlenden Ausübung der informationellen Selbstbestimmung von Art. 6 Abs. 1 lit b. DSGVO gerade nicht erfasst sind. Siehe hierzu Buchner/Petri in Kühling/Buchner: DS-GVO, 1. Aufl. (2017), Art. 6 Rn. 29-31.

Sachverhalt

Das Angebot der SCHUFA beinhaltet einen Auskunftsservice zu den, bei der SCHUFA gespeicherten, Bonitäts- und Identitätsdaten, vorformulierte Formulare sowie den Identitätsschutz. Der Identitätsschutz umfasst den IdentSafe-Monitor zur Überwachung der Daten im Internet sowie im Deep Web und Darknet, die IdentSafe-Hotline, den IdentSafe-Cleaner zur Entfernung unerwünschter Einträge im Internet und den IdentSafe-Schlüsselservice zur Rücksendung gefundener Schlüssel.[101] Da letzteres in Bezug auf digitale Identitäten nicht relevant ist, wird hierauf nicht weiter eingegangen.

Die Nutzung von meineSCHUFA plus setzt eine Registrierung im meineSCHUFA-Portal sowie den Abschluss eines kostenpflichtigen Nutzungsvertrages für die Zusatzleistungen voraus. Im Rahmen der Registrierung erfolgt eine Identifikation der Interessenten mittels Personalausweis oder PostIdent-Verfahren. Der Benutzername wird daraufhin per E-Mail und weitere Zugangsdaten werden per Post oder ePostbrief an den Kunden versendet. Nach Erhalt dieser Daten kann der Kunde sich einloggen und die Suchdaten in verschiedenen Rubriken ergänzen. Mögliche Kategorien sind Name, Geburtsdatum, Telefon, Kreditkarten und Ausweisnummern, E-Mail-Adressen und Kontodaten.[102] Der IdentSafe-Monitor sucht einmal täglich nach diesen Daten sowie nach spezifischen nicht näher beschriebenen Kombinationen. Die Kombinationen werden durch den IdentSafe-Monitor festgelegt und können nicht geändert werden. Werden entsprechende Daten entdeckt, entscheidet ein Algorithmus ob hierdurch ein Risiko für die Identität des Kunden besteht. Ist dies der Fall, bekommt der Kunde direkt eine Nachricht per E-Mail oder SMS.[103] In allen anderen Fällen erhält der Kunde alle 90 Tage einen Bericht mit einer Übersicht über alle Suchergebnisse in diesem Zeitraum.[104] Eine Garantie in Bezug auf Vollständigkeit und Richtigkeit der Suchergebnisse gibt es nicht.

Der IdentSafe-Cleaner kann bei entsprechenden Funden verwendet werden um die Löschung der Einträge in die Wege zu leiten. Dies gilt für alle durch den IdentSafe-Monitor abgedeckte Seiten sowie diverse Suchmaschinen. Die Beauftragung hierzu erfolgt mittels eines im Nutzerbereich verfügbaren Musterformulars.

---

[101] SCHUFA: Die Leistungen von meineSCHUFA plus, über: https://www.meineschufa.de/index.php?site=22_1&via=menu (abgerufen am 19.07.2018).
[102] Pressemitteilung SCHUFA: Mehr Sicherheit im Netz mit SCHUFA IdentSafe vom 16.02.2012, über: https://www.schufa.de/de/ueber-uns/presse/pressemitteilungen/schufa-identsafe.jsp (abgerufen am 19.07.18).
[103] SCHUFA: Allgemeine Geschäftsbedingungen und Hinweise für die SCHUFA Privatkundenprodukte (Stand Mai 2018), über: https://www.meineschufa.de/downloads/agb.pdf (abgerufen am 24.07.2018), S. 3.
[104] SCHUFA: AGB, S. 3.

Eine Registrierung weiterer Nutzer ist in diesem Paket nicht möglich. Es kann lediglich in den meineSCHUFA premium-Tarif gewechselt werden. Hier ist dann die Registrierung eines weiteren Nutzers möglich.[105]

Die verfügbare Datenschutzerklärung umfasst jede Form der Datenverarbeitung durch die SCHUFA. Einzelangaben zur konkreten Datenverarbeitung im Rahmen des IdentSafe-Verfahrens gibt es nicht.

Im Abschnitt 2.1 über die Zwecke der Datenverarbeitung schreibt die SCHUFA jedoch ausdrücklich, dass personenbezogene Daten, die der Identifizierung des Nutzers dienen auch genutzt werden um den Datenbestand der SCHUFA über diese Person zu aktualisieren.[106] Außerdem werden zur Aufgabenerfüllung Daten an IT-Dienstleister weitergegeben.[107]

Schlussfolgerungen

Da die Datenschutzinformation der SCHUFA keine gesonderten Hinweise für die Datenverarbeitung des IdentSafe-Verfahrens enthält, ist anzunehmen, dass die hier getroffenen allgemeinen Angaben grundsätzlich auch auf diese Dienstleistung Anwendung finden.

Transparenz

Aus den AGB und der Datenschutzerklärung lassen sich kaum konkrete Aussagen zum IdentSafe-Schutz ablesen. Hiernach wird die Verarbeitung personenbezogener Daten auf drei Erlaubnistatbestände – Einwilligung, Vertragserfüllung, berechtigtes Interesse – gestützt. Es wird nach den vom Kunden gewünschten Daten aus bestimmten Rubriken sowohl im Surfaceweb als auch im Deepweb und Darknet gesucht. Ob diese Suche durch einen Dienstleister, einen Auftragsverarbeiter oder die SCHUFA selbst durchgeführt wird, ist nicht bekannt. Da die SCHUFA jedoch ausdrücklich auf die Datenübermittlung zu Vertragspartnern hinweist, ist es wahrscheinlich, dass die Suche nicht durch die SCHUFA selbst erfolgt. Auch über die Funktionsweise des Suchalgorithmus und die von diesem festgelegten kritischen Kombinationen ist nichts bekannt, ebenso wenig über die Kriterien die zur Risikobewertung herangezogen werden.

Wie beim Versicherungsmodell (s.o.) wird nicht darauf eingegangen wie mit Informationen verfahren wird, die nicht unter die Kategorie unberechtigter Veröffentlichungen fallen.

---

[105] SCHUFA: meineSCHUFA premium, über: https://www.meineschufa.de/index.php?site=22_1_2&via=menu (abgerufen am 24.07.2018).
[106] SCHUFA: Datenschutzinformation nach Art. 13 DS-GVO (Stand Mai 2018), über: https://www.meineschufa.de/index.php?site=datenschutz (abgerufen am 23.07.2018).
[107] SCHUFA: Datenschutzinformation.

Verfügbarkeit

Der „Quartalsbericht" enthält alle Fundstellen, die in einem 90 Tage Zeitraum erfasst wurden. Über den Detailgrad der Berichte ist nichts bekannt. Der Kunde erhält außerdem den Schriftverkehr zwischen Seitenbetreibern und der SCHUFA zu allen Lösch- und Sperraufträgen. Was konkret in den Berichten bzw. in den Alarmmeldungen enthalten ist, ist nicht bekannt.

Unklar ist auch wie lange die SCHUFA die Daten zu den Suchergebnissen speichert. In der Datenschutzinformation heißt es jedoch: *„Wir verfolgen daneben der Grundsatz, Daten zur werblichen Nutzung nach 4 Jahren nach Vertragsende bzw. nach 4 Jahren nach Ende der Marketingbemühungen zu löschen."*[108] Daher kann angenommen werden, dass insbesondere personenbezogene Daten, die aufgrund berechtigter Interessen verarbeitet wurden, über das Vertragende hinaus gespeichert werden. Dauerhaft gespeichert bleiben jedenfalls die Daten, die im Rahmen der Authentifizierung des Nutzers zur Ergänzung des SCHUFA-Datenbestands weiterverarbeitet wurden. Welche Auswirkungen dies auf den SCHUFA-Score hat, ist nicht bekannt, da die Methode der Scorewertberechnung Geschäftsgeheimnis der SCHUFA ist.

Vertraulichkeit

Der IdentSafe-Monitor überwacht die vom Nutzer zur Verfügung gestellten personenbezogenen Daten tagesaktuell, führt alle Fundstellen in einem Bericht zusammen und übermittelt diesen per E-Mail. Da E-Mails in der Regel unverschlüsselt übermittelt werden, besteht hier – abhängig von Inhalt der E-Mail – ein weiteres Risiko für einen Bruch der Vertraulichkeit.

Grundsätzlich positiv zu bewerten ist, dass eine Authentifizierung des Nutzers erforderlich ist um das Angebot überhaupt in Anspruch nehmen zu können. Hierdurch wird die Möglichkeit nach Daten Dritter suchen zulassen erheblich eingeschränkt. Auch das die Zugangsdaten per Post und nicht unverschlüsselt via E-Mail an den Nutzer geschickt werden, ist positiv hervorzuheben. Die Verarbeitung zu anderen als den ursprünglichen Zwecken ist jedoch zu kritisieren, da die SCHUFA sich hierüber das Recht herausnimmt ihren Datenbestand zu aktualisieren. Erstens ist fraglich ob die Zweckänderung überhaupt zulässig ist. Zweitens besteht für den Kunden keine Möglichkeit die Nutzung der Daten aus dem Identifizierungsschritt zu verhindern, da ein Widerspruch gegen die Datennutzung zwar vorgesehen, aber nur nachträglich und auch nur separat möglich ist. Dem Betroffenen bleibt also nur von der Dienstleistung abzusehen.

[108] SCHUFA: Datenschutzinformation, S. 3.

Intervenierbarkeit

In der Datenschutzinformation wird unter Nr. 3 auf die Betroffenenrechte nach Art. 15-18, 20 und 21 DSGVO verwiesen.[109] Es werden die verschiedenen Kontaktmöglichkeiten zur Durchsetzung von Lösch- und Berichtigungsanträgen genannt.

Löschansprüche, die sich aus den vom IdentSafe-Monitor ermittelten Fundstellen ergeben, können mit Hilfe des IdentSafe-Cleaners gegenüber den Seiten bzw. Suchmaschinenbetreibern durchgesetzt werden.[110]

Im Falle eines Identitätsdiebstahls können Betroffene dies bei der SCHUFA melden. Diese Information wird zum SCHUFA-Datenbestand und zu einem gesonderten SCHUFA-Fraudpool hinzugespeichert. Dies soll die Verwendung der gestohlen Identitätsdaten erschweren. Inwiefern diese Einmeldung von Identitätsbetrug durch die Verwendung des Monitors den Betroffenen nahegelegt wird, ist aus den vorliegenden Informationen nicht ersichtlich.

Integrität

Für die Vollständigkeit und Richtigkeit der gefundenen Daten kann die SCHUFA nicht garantieren.[111] Die Aktualität der Suchdaten obliegt dem Kunden, da dieser die entsprechenden Parameter vorgibt.

Unverkettbarkeit

Der IdentSafe-Monitor sucht nach bestimmten Kombinationen personenbezogener Daten. Um welche es sich hierbei genau handelt, ist nicht bekannt. In den AGB ist hierzu vermerkt, dass bei Funden, die die „Identität diskreditieren oder verfälschen könnten", der Algorithmus eine Warnmeldung auslöst. Zumindest die Suche beinhaltet daher eine Verkettung verschiedener personenbezogener Daten. Darüber hinaus ergibt sich auch aus den regelmäßigen Berichten, in denen alle Fundstellen zusammengefasst werden, eine Verkettung. Da der Scoring-Algorithmus der SCHUFA ein Geschäftsgeheimnis ist - also nicht bekannt ist welche Faktoren in die Berechnung einfließen - ist es denkbar, dass auf diesem Weg gewonnene Erkenntnisse, z.B. besonders viele Warnmeldungen, sich negativ auf den Scorewert auswirken. Ein Betroffener, dessen Daten häufig im Internet veröffentlicht werden, wird möglicherweise als eher fahrlässig um Umgang mit seinen Daten eigestuft und dies führt in der Folge zu einem erhöhten Risiko für Banken und Versicherungen für Kosten für Folgeschäden aufkommen zu müssen bzw. zu einem höheren Arbeitsaufwand.

[109] SCHUFA: AGB, S. 3.
[110] SCHUFA: AGB, S. 3f.
[111] SCHUFA: AGB, S. 3.

3.3.4 Dienstleister

Owl-Detect ist ein Produkt des Sicherheitsdienstleisters CPP. Die Dienstleistung kann von Privatkunden direkt vom Anbieter bezogen werden, steht jedoch auch als Ergänzung des Portfolios für beispielsweise Banken und Versicherungen zur Verfügung. Der hier erfolgten Analyse liegt der Direktbezug der Dienstleistung durch den Kunden zu Grunde. Es handelt sich ebenfalls um einen Monitoring-Service.

Sachverhalt

Owl Detect sucht 24 Stunden am Tag/sieben Tage die Woche nach den vom Kunden festgelegten Daten. Möglich ist die Überwachung je einer Reisepass-, Personalausweis-, Krankenversicherten- und Führerscheinnummer. Außerdem können je 10 Kontonummern, Kreditkarten, E-Mail-Adressen und Telefonnummern überwacht werden. Eine Authentifizierung der angegebenen Daten erfolgt nicht.

Nach der Anmeldung kann der Kunde die gewünschten Daten im Nutzerkonto hinterlegen. Die erste Maßnahme ist ein Abgleich der Daten mit der Owl Detect-Datenbank. Rückwirkend für sechs Jahre wird überprüft, ob die Daten bereits kompromittiert wurden. Sollte sich dies bestätigen, erhält der Kunde bereits zu diesem Zeitpunkt die erste Warnmeldung.

Im weiteren Verlauf werden die angegebenen Daten regelmäßig mit der Datenbank abgeglichen: *„Wir durchsuchen keine externen Quellen speziell nach Ihren persönlichen Daten. Wenn wir das Darknet scannen, suchen wir nach angebotenen personenbezogenen Daten, die wir in unsere Systeme laden und so sicher mit den Angaben abgleichen können, die Owl für Sie überwacht."*[112]

Überwacht wird von Owl Detect explizit nur das Darknet (Datensenken). Abgleiche mit dem Surface Web erfolgen nicht. Der IT-Dienstleister CSID überwacht die Daten im Rahmen eines Auftragsverarbeitungsvertrags und hostet zu diesem Zweck die Suchdaten der Kunden auf Servern in Großbritannien.[113] Der Kunde erhält eine Benachrichtigung, wenn es eine Übereinstimmung der überwachten Daten mit der Datenbank des Auftragsverarbeiters gibt. Ein Anspruch auf Vollständigkeit besteht nicht und es gibt auch kein Zeitfenster innerhalb dessen eine Benachrichtigung garantiert wird. Die Meldung informiert den Kunden auch nicht darüber, wo die Daten gefunden wurden.

Sollte es Übereinstimmungen geben, wird der Kunde via E-Mail und/oder SMS benachrichtigt. Einmal im Monat erhält der Kunde außerdem einen Bericht zu allen Ereignissen. Im Nutzerkonto kann jederzeit Einsicht in den aktuellen Stand genommen und im Falle eines Fundes auf den Maßnahmenplan zugegriffen werden. Dieser enthält Empfehlungen, welche

[112] Owl Detect: FAQs Datenübermittlung, über: https://www.owldetect.de/faqs/ (abgerufen am 26.07.2018).
[113] Owl Detect: Allgemeine Geschäftsbedingungen, über: https://www.owldetect.de/agb/ (abgerufen am 27.07.2018), Abschnitt B.

Aktionen im Falle einer Meldung zu treffen sind. Hierbei handelt es sich um allgemeine Hinweise, die nicht notwendiger Weise auf den konkreten Einzelfall anwendbar sein müssen.[114]

Die Daten werden solange gespeichert, wie der Vertrag zwischen dem Kunden und dem Anbieter besteht.[115]

Schlussfolgerungen

Vertraulichkeit

Es gibt keine Angaben darüber, wie verhindert werden soll, dass ein Kunde personenbezogene Daten Dritter als Suchdaten angibt.

Zu bemängeln ist auch, dass alle Telefongespräche aufgezeichnet werden und offenbar keine Möglichkeit eines Opt-out besteht.[116] Da Informationen zur Meldung auch telefonisch abgerufen werden können, werden in einem solchen Fall sensible Daten dauerhaft gespeichert – es ist keine Löschfrist angegeben - und die Daten für einen anderen als den ursprünglichen Zweck genutzt. Es ist zudem fraglich, welche gesetzlichen und behördlichen Vorgaben durch die Mitschnitte erfüllt werden sollen.

Verfügbarkeit

Im Gegensatz zum Modell der Versicherung bzw. der Auskunftei wird die Vorgehensweise zum Datenabgleich bei Owl erläutert. In den AGB wird eine „Datenbank gefährdeter persönlicher Daten“[117] genannt mit der die vom Kunden zur Überwachung angegebenen Daten abgeglichen werden. Die Datenbank ermöglicht zudem die Daten von Neukunden Rückwirken für sechs Jahre zu prüfen. Daraus folgt, dass Owl Detect einmal erhobene Daten mindestens für diesen Zeitraum speichert. Da die Verjährungsfrist für zivilrechtliche Ansprüche des Betroffenen regelmäßig auf drei Jahre begrenzt ist (§ 195 BGB), könnte im Sinne der Datenminimierung eine kürzere Speicherdauer ausreichend sein.

Transparenz

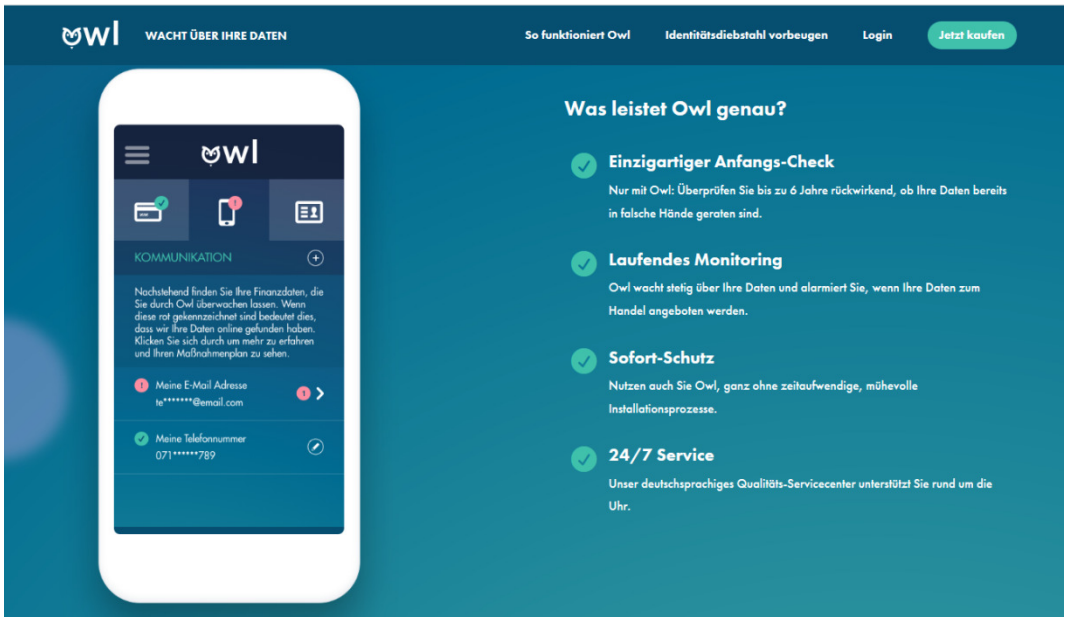
Die Informationen zur Datenverarbeitung sind sowohl in den AGB als auch in der Datenschutzrichtlinie übersichtlich dargestellt und öffentlich zugänglich. Auf die einzelnen Verfahren zur Datenverarbeitung, insbesondere zum Identitätsschutz, wird ausdrücklich Bezug

[114] Siehe hierzu Owl Detect: So funtioniert Owl, über: https://www.owldetect.de/so-funktioniert-owl/ (abgerufen am 27.07.2018) und Owl Detect: AGB.
[115] Owl Detect: Datenschutzrichtlinie und Cookie Policy, über: https://www.owldetect.de/datenschutzrichtlinie-und-cookie-policy/ (abgerufen am 27.07.2018).
[116] Owl Detect: AGB, Abschnitt A § 12.
[117] Owl Detect: AGB, Abschnitt B §1.

genommen. Die Zwecke sind klar definiert und die im Nutzerkonto bereitgestellten Daten werden nicht zweckändernd auf Grund eines berechtigten Interesses weiterverarbeitet.

Aus den AGB bzw. der Datenschutzrichtlinie ist nicht ersichtlich, dass die Anfangsüberprüfung rückwirkend für sechs Jahre die Daten überprüft werden. Mit dieser Information wird jedoch auf der Webseite des Anbieters geworben (Abb. 4).[118]

Abb. 4 Leistungsübersicht



Intervenierbarkeit

In den AGB ist zur Datenübertragbarkeit vermerkt, dass die Herausgabe bzw. Übertragung der Daten nicht erfolgt soweit die Rechte und Freiheiten anderer Personen oder auch des Unternehmens dadurch beeinträchtigt würden. Eine solche Beschränkung zu Gunsten von Unternehmen sieht Art. 20 DSGVO jedoch nicht vor. Zweck der Norm ist auch die Förderung des Wettbewerbs. Die Übermittlung der personenbezogenen Daten an einen anderen Anbieter soll vereinfacht werden und die Kunden somit zum Anbieterwechsel animiert werden. Ein vertraglicher Ausschluss der Übermittlung würde diesen Effekt untergraben und die Norm in Leere laufen lassen.[119] Eine Schranke des Rechts auf Datenübertragbarkeit findet sich in Absatz 3, der auf die Datenverarbeitung gemäß Art. 6 Abs. 1 lit. e) DSGVO, also öffentliche Stellen, verweist. Zwar spricht die Norm selbst in Abs. 4 nur von anderen Personen, Erwägungsgrund 68 präzisiert Art. 20 Abs. 4 DSGVO jedoch eindeutig. Hier ist aus-

[118] Vgl. https://www.owldetect.de/ (abgerufen am 12.10.18).
[119] Herbst in: Kühling/Buchner, DSGVO, 1.Aufl. 2017, Art. 20 Rn. 22.

drücklich von den Grundrechten und Freiheiten betroffener Personen die Rede. Das Unternehmen als verantwortliche Stelle profitiert damit nicht von der Norm.[120]

Verkettbarkeit

Die zum Abgleich der zu überwachenden Daten verwendete Datenbank reicht mindestens sechs Jahre zurück. Hier besteht ein entsprechend großes Verkettungspotential. Aufgrund der bei Owl Detect möglichen 44 Einzelangaben könnte somit ein umfassendes Nutzerprofil erzeugt werden. Zusätzlich besteht die Möglichkeit, dass über diesen langen Zeitraum einzelne Angaben einer anderen Person zuzuordnen waren. Insbesondere E-Mail-Adressen und Telefonnummern, aber auch Kontonummern werden neu vergeben. Hier kann es daher zu falsch-positiven Ergebnissen kommen.

Integrität

Wie die anderen Anbieter auch gibt Owl Detect keine Garantie für die Vollständigkeit der Funde. Es findet ausdrücklich keine Überprüfung der überwachten Daten statt.[121]

3.3.5 Forschungsinstitut

Das Hasso-Plattner-Institut (HPI) bietet einen Dienst (HPI Leak Checker) an mit dessen Hilfe Nutzer überprüfen können, ob ihre E-Mail-Adresse und damit ggf. auch anderen (sensible) personenbezogene Daten im Internet öffentlich auffindbar sind.[122] Zum Zeitpunkt der Erstellung dieses Dokument waren etwas mehr als 5,8 Mrd. geleakte Nutzerkonten vom Dienst erfasst.[123] Zusätzlich zu den Nutzerkonten wertet der Dienst auch die Häufigkeiten der in den Leaks enthaltenen Klartextpasswörter aus.

Sachverhalt

Der Nutzer kann seine E-Mail-Adresse in eine Suchmaske eingeben. Man erhält in jedem Fall eine Benachrichtigung an die angegebene E-Mail-Adresse zum Ergebnis der Suche. Entweder es handelt sich hierbei um die Nachricht, dass in der HPI-Datenbank kein passender Eintrag gefunden wurde (Abb. 5) [124] oder der Nutzer erhält eine E-Mail, die über den entsprechenden Fund informiert. In letzterem Fall enthält die Benachrichtigung Informationen zum Leak (Name/Link) und zu den betroffenen und nicht betroffenen Datenkategorien (Abb. 6)[125].

[120] Siehe auch BeckOK DatenschutzR/von Lewinski, 24. Ed. 1.5.2018, DS-GVO Art. 20 Rn. 109; Paal in Paal/ Pauly: Datenschutz-Grundverordnung, 2017, Art. 20 Rn. 24.
[121] Owl Detect: AGB, Abschnitt B §1.
[122] HPI: Startseite, über: https://sec.hpi.de/ilc/search (abgerufen am 07.08.2018).
[123] HPI: Statistiken, über: https://sec.hpi.de/ilc/statistics (abgerufen am 07.08.2018).
[124] HPI: Antwort-E-Mails, über: https://sec.hpi.de/ilc/publickeys (abgerufen am 07.08.2018).
[125] HPI: Antwort-E-Mails, über: https://sec.hpi.de/ilc/publickeys (abgerufen am 07.08.2018).

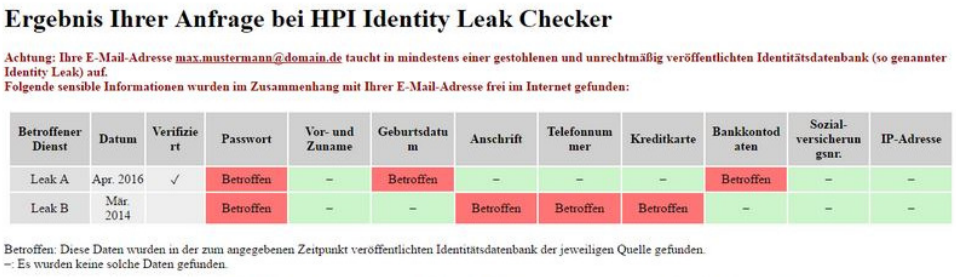
Abb. 5 Negatives Ergebnis

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Glückwunsch: Ihre E-Mail-Adresse max.mustermann@domain.de taucht nicht in unserer Datenbank auf. Das garantiert jedoch nicht, dass keine Ihrer persönlichen Informationen gestohlen wurden.

Die Benachrichtigung enthält außerdem Informationen zum (vermutlichen) Alter des Leaks und ob dieser vom Dienstanbieter oder aufgrund belastbarer Indizien bestätigt wurde – es sich also tatsächlich um einen Datenschutzvorfall handelt und nicht nur um eine Kombination alter Leaks oder fingierte Daten.[126]

Abb. 6 Positives Ergebnis



Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse max.mustermann@domain.de taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.
Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozialversicherungsnr.	IP-Adresse
Leak A	Apr. 2016	✓	Betroffen	–	Betroffen	–	–	–	Betroffen	–	–
Leak B	Mär. 2014		Betroffen	–	–	Betroffen	Betroffen	Betroffen	–	–	–

Betroffen: Diese Daten wurden in der zum angegebenen Zeitpunkt veröffentlichten Identitätsdatenbank der jeweiligen Quelle gefunden.
–: Es wurden keine solche Daten gefunden.

Die Nachricht verweist im Haftungsauschluss darauf, dass nur online verfügbare Datenquellen ausgewertet werden. Nähere Angaben zu den in der jeweiligen Kategorie eingetragenen Daten erbringt der Dienst liefert der Dienst aus Datenschutzgründen nicht.

In Bezug auf die Frage, in welcher Form die geleakten Daten gespeichert werden, gibt HPI zudem an, dass die Daten tatsächlich nicht gespeichert sind. Es werden lediglich die betroffenen Kategorien erfasst. Die E-Mail-Adresse wird nicht im Klartext sondern als Hashwert gespeichert. Im Rahmen der Abfrage wird die eingetragene Adresse ebenfalls mit dem verwendeten Hash-Algorithmus umgerechnet und mit der Datenbank abgeglichen. Die automatisch generierte Antwort ist mit einem OpenPGP-Schlüssel signiert, der zur Adresse *sec-checker-admin(at)hpi.de* gehört.[127]

Schlussfolgerungen

Verfügbarkeit

Der Nutzer erhält einige zusätzliche Informationen sowohl zum Data Breach als auch zu den betroffenen Datenkategorien. Die Informationen werden in Form einer Tabelle zusammengefasst. Die betroffenen Datenkategorien sind rot gekennzeichnet, die die nicht im Leak vorhanden waren grün. Nicht ersichtlich ist, ob in einem Leak enthaltene Passwörter im

[126] HPI: Antwort-E-Mails.
[127] HPI: Antwort-E-Mails.

Klartext oder verschlüsselt vorlagen. Diese Information kann bei einem verifizierten Leak unter Umständen vom Verantwortlichen zur Verfügung gestellt werden, müsste aber ggf. vom Betroffenen recherchiert werden. Vermutlich wird auf diese Angabe verzichtet um einen bestimmten Leak nicht unnötig attraktiver für weitere Angreifer zu machen. In Bezug auf das Risiko ist dies für den Betroffenen jedoch eine wichtige Information. Dessen Bereitschaft das Passwort zu ändern wird bei einem öffentlich im Klartext verfügbaren Passwort bestärkt werden.

Intervenierbarkeit und Transparenz

Die Datenschutzerklärung ist mit nur vier Unterpunkten sehr knapp gehalten. Die Angaben der Datenschutzerklärung zur Datenverarbeitung beschreiben nicht den vollen Umfang des Angebots. So fehlen beispielsweise grundlegende Angaben zur Speicherdauer, Art und Umfang der Erhebung sowie zur Weiterverarbeitung der Daten, wie zum Beispiel für die Übersicht zu den Klartextpasswörtern. Es wird nicht explizit erwähnt auf welcher Rechtsgrundlage die Verarbeitung überhaupt erfolgt.

In der Datenschutzerklärung sind zu den Betroffenenrechten lediglich zwei Punkte aufgeführt. Der Betroffene hat demnach keinen Anspruch auf Auskunft nach Art. 15 DSGVO, soll jedoch die Auskünfte zur entsprechenden Adresse sperren und löschen können. Wie genau dieser Sperr- bzw. Löschanspruch durchsetzbar ist, wird allerdings nicht beschrieben.[128] Warum der Anspruch auf Auskunft nicht gegeben sein soll, ist unverständlich, denn diese Funktion erfüllt die Suchfunktion des Leak Checkers bereits teilweise. Für jeden Auskunftsanspruch muss der Betroffene einen Identifikator zur Verfügung stellen – im vorliegenden Fall die E-Mail-Adresse – damit der Verantwortliche weiß, wonach gesucht werden soll. Hintergrund ist wahrscheinlich, dass es keinen Identitätsnachweis des Ersuchenden gibt und somit nicht sichergestellt werden kann, dass es sich tatsächlich um den Betroffenen handelt. Eine Verweigerung jeglicher Auskünfte ist dadurch jedoch nicht zu rechtfertigen. Diese Schwachstelle hindert HPI zudem nicht daran den eigentlichen Service zu betreiben und die - via **unverschlüsselter** E-Mail übermittelten - Informationen bereitzustellen. Hier wird darauf vertraut, dass der Empfänger die Kontrolle über das E-Mail-Postfach besitzt und somit berechtigter Empfänger der Informationen (Betroffener) ist. Es wäre durchaus möglich dem Betroffenen seine/ihre Daten gemäß Art. 15 DSGVO zugänglich zu machen, indem der Verantwortliche auf der Grundlage der Kontrolle über das E-Mail-Postfach die Auskunft erteilt. Hierfür müssten ggf. zusätzliche entsprechende Schutzmaßnahmen implementiert werden, wie bespielweise die Bestätigung eines Links, die Eingabe einer PIN oder Ende-zu-Ende-verschlüsselte Kommunikation.[129] Denkbar wäre auch, dass nur Teile der

[128] HPI: Datenschutzerklärung, über: https://sec.hpi.de/ilc/dataprivacy (abgerufen am 08.08.2018).
[129] Vgl DSK: Kurzpapier Nr. 6 – Auskunftsrecht der Betroffenen Person, über: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_6_Auskunftsrecht.pdf (abgerufen am 15.08.2018) sowie DSGVO (EW 63).

enthaltenen personenbezogenen Daten übermittelt werden, wenn die Sicherheit des Kommunikationskanals nicht gewährleistet werden kann. Es fehlt auch der Hinweis auf ein Widerspruchsrecht nach Art. 21 DSGVO.

Punkt drei und vier der Datenschutzerklärung beziehen sich nicht auf den Leak Checker sondern informieren zur Datenerhebung auf der Webseite und durch Drittanbieter.[130]

Vertraulichkeit

Wie oben bereits beschrieben wird die Vertraulichkeit der Daten dadurch gewährleistet, dass das Ergebnis des Leak Checks mittels unverschlüsselter E-Mail an die eingegebene E-Mail-Adresse versandt wird.

Die E-Mail-Adresse ist nur als Hash-Wert in der Datenbank hinterlegt. Die Datenbank enthält zudem nur Angaben darüber, ob in einem Leak in einer bestimmten Datenkategorie ein Wert hinterlegt war. Ein Angreifer der sich Zugriff auf diese Datenbank verschafft, erhält demnach nur die Information, dass ein Passwort vorhanden war, kann jedoch nicht feststellen welches.[131]

Wie die personenbezogenen Daten gegen interne Angreifer geschützt werden, ist nicht beschrieben.

Integrität

Da die E-Mail signiert ist, kann der Nutzer - sofern die erforderlichen Komponenten vorhanden sind - den Ursprung der Nachricht verifizieren und darauf vertrauen, dass der Inhalt nicht verändert wurde. Der öffentliche Schlüssel ist auf der Webseite verfügbar.

Eine Garantie dafür, dass die geleakten Daten vollständig und richtig sind, gibt es nicht.

Verkettbarkeit

Aufgrund der fehlenden Löschroutinen ist das Verkettungspotential umso größer, je länger der Dienst angeboten wird. Hierbei wird zudem außer Acht gelassen, dass E-Mail-Adressen nicht lebenslang vergeben werden. Insbesondere bei Funktionsadressen ist dies kritisch, aber auch private Nutzer könnten so an personenbezogene Daten Dritter gelangen.

3.3.6 Staatliche Stelle

Der BSI-Sicherheitstest wird vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) zur Verfügung gestellt. Hintergrund für die Implementierung des Service war ein Ermittlungsverfahren der Staatsanwaltschaft Verden im Zuge dessen der potentielle Daten-

[130] HPI: Datenschutzerklärung.
[131] HPI: In welcher Form sind die geleakten Daten gespeichert?, über: https://sec.hpi.de/ilc/about (abgerufen am 08.08.2018).

missbrauch von E-Mail-Adressen und Passwörtern mehrerer Millionen Bürger entdeckt wurde. Um auch die Betroffenen zu benachrichtigen, die nicht über die großen Telekommunikationsanbieter erreicht werden konnten, wurde der BSI-Sicherheitstest eingerichtet.

Sachverhalt

Der Nutzer kann seine E-Mail-Adresse über den BSI-Sicherheitstest mit der Datenbank des BSI abgleichen. Hierzu trägt der Nutzer die entsprechende Adresse in das Suchfeld ein und startet die Überprüfung (Abb. 7)[132]. Gegebenenfalls ist noch ein Captcha einzutragen. Im Anschluss daran wird dem Nutzer ein vierstelliger „Betreff-Code" angezeigt. Dieser wird in der Betreffzeile der Benachrichtigung angezeigt, sollte die eingegebene E-Mail-Adresse betroffen sein. Im Falle eines Fundes wird die Warnung an die entsprechende E-Mail-Adresse versandt. Eine Speicherung der gesuchten Adresse über den Sicherheitstest hinaus findet nicht statt.

Schlussfolgerungen

Transparenz

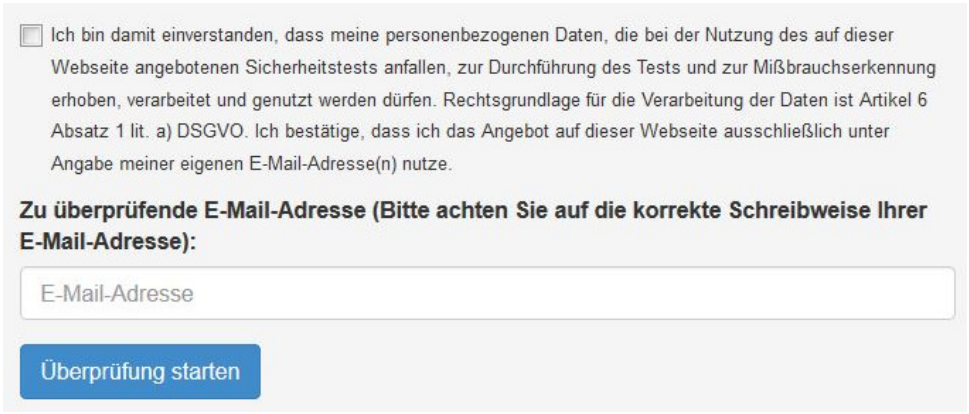
In der Datenschutzerklärung sind z.T. Passagen enthalten, die Sachverhalte regulieren, die für das BSI gar nicht einschlägig sind. Hierzu zählt beispielsweise der Hinweis auf ein Widerspruchsrecht gegen Direktwerbung nach Art. 21 Abs. 2 ff DSGVO.[133] An der Datenschutzerklärung zu kritisieren ist auch die Berufung des BSI auf Art. 6 Abs. 1 lit. f) DSGVO. Es ist unverständlich, welche weiteren berechtigten Interessen an einer Datenverarbeitung über die vom Gesetzgeber vorgesehenen Kompetenzen hinaus das BSI (als Behörde) geltend machen möchte, zumal Art. 6 Abs. 1 UAbs. 2 DSGVO sowie ErwG 47 deutlich darauf verweisen, dass Art. 6 Abs. 1 lit. f) DSGVO nicht für Verarbeitungen im Rahmen der Aufgabenerfüllung von Behörden gilt.

Die Verarbeitung der E-Mail-Adressen im Sicherheitstest basiert jedoch ausweislich (Abb. 7)[134] auf der Einwilligung des Nutzers gemäß Art. 6 Abs. 1 lit. a) DSGVO.[135]

---

[132] BSI: https://www.sicherheitstest.bsi.de (07.08.2018).
[133] BSI: Datenschutzerklärung; Nr. 6, über: https://www.sicherheitstest.bsi.de/datenschutzerklaerung (abgerufen am 07.08.2018).
[134] BSI: https://www.sicherheitstest.bsi.de (07.08.2018).
[135] BSI: Datenschutzerklärung, über: https://www.sicherheitstest.bsi.de/datenschutzerklaerung (abgerufen am 06.08.2018).

Abb. 7 BSI-Sicherheitstest



Vertraulichkeit

Der BSI-Sicherheitstest kann völlig anonym genutzt werden, d.h. es findet keine Verifikation der Identität des Nutzers statt. Jeder kann jede E-Mail-Adresse eingeben, auch wenn der Nutzer „versprechen" muss, dass nur die eigenen E-Mail-Adressen geprüft werden (Abb. 7). Technisch verhindert wird die Eingabe fremder E-Mail-Adressen nicht. Die Vertraulichkeit der Funde wird dadurch gewährleistet, dass kein direktes Feedback an den Nutzer über die Webseite ausgegeben wird. Sollte eine E-Mail-Adresse betroffen sein, erfährt der Nutzer dies über eine entsprechende Benachrichtigungs-E-Mail. Der dahinter stehende Ansatz ist, dass nur derjenige, der Zugriff auf das E-Mail-Postfach hat, Informationen über einen möglichen Datenmissbrauch erhält. So wird sichergestellt, dass Nutzern, die nicht ihre eigene E-Mail-Adresse eingeben, keine weiteren Informationen offenbart werden. Die Kommunikation erfolgt allerdings ausschließlich mittels unverschlüsselter E-Mail-Kommunikation.

Integrität

Die Integrität der Benachrichtigung wird einerseits durch den vierstelligen Betreff-Code und andererseits durch die Signierung der E-Mail mittels OpenPGP-Zertifikat sichergestellt.

Die Signierung der E-Mail dient dazu, dass der Nutzer sicher gehen kann, dass die E-Mail tatsächlich vom BSI stammt. Nicht erwähnt, aber über diesen Weg ebenfalls auch möglich, ist eine Integritätsprüfung des Inhalts. Der öffentliche Schlüssel kann direkt über die Webseite heruntergeladen werden.[136] Da die Nutzung des OpenPGP-Standards nicht ausreichend verbreitet ist und nicht jeder Nutzer über die erforderlichen Komponenten zur Überprüfung der Signatur verfügt, wird der Betreff-Code als zusätzliche Authentifizierungsmethode verwendet. Damit ist dann nicht nur bestätigt, dass die E-Mail vom BSI stammt sondern auch, dass der Inhalt der E-Mail nicht verändert wurde.

[136] https://www.sicherheitstest.bsi.de/gpg

Verfügbarkeit

Die über den BSI-Sicherheitstest abrufbaren Informationen beziehen sich nur auf einen bestimmten Vorfall aus dem Jahr 2016. In Zusammenhang mit dem Ermittlungsverfahren zur Botnetzinfrastruktur „Avalanche“ wurden die Betroffenen zum Teil von ihrem Telekommunikationsanbieter benachrichtigt.[137] Für alle Betroffenen, die auf diese Weise nicht informiert werden konnten, stellte das BSI den Sicherheitstest bereit. Es ist somit davon auszugehen, dass das BSI im Rahmen seiner Kompetenzen nur im konkreten Einzelfall die Datenbank aktualisiert. Gemäß des IT-Sicherheitsgesetzes umfasst dies vor allem Bedrohungen kritischer Infrastrukturen und damit verbunden die Warnung der Öffentlichkeit nach § 7 Abs. 1 S. 1 Nr. 1 c) ITSiG.

Der Betroffene wird durch die Benachrichtigung per E-Mail darüber in Kenntnis gesetzt, dass die im BSI-Sicherheitstest eingegebene E-Mail und ein Passwort in dem Leak enthalten sind. Weitere Informationen – ob beispielsweise auch Kontodaten, Adressen oder ähnliches enthalten waren – werden nicht mitgeteilt. Sobald der Test abgeschlossen ist, werden die zur Durchführung des Tests erhobenen Daten (die E-Mail-Adresse) wieder gelöscht.

Verkettbarkeit

Aufgrund der Tatsache, dass das BSI nur sporadisch neue Leaks für eine öffentliche Suche zur Verfügung stellt und keine direkte Rückmeldung zur Betroffenheit erfolgt, sind Möglichkeiten der Verkettung, wenn überhaupt nur sehr begrenzt gegeben. Dies ist insbesondere dann der Fall, wenn eine E-Mail-Adresse in der Zwischenzeit neu vergeben wurde oder von mehr als einer Person verwendet wird (Familienadresse, Funktionsadressen).

Intervenierbarkeit

In der Datenschutzerklärung wird auf die in der DSGVO dargelegten Betroffenenrechte hingewiesen. Entsprechend kann ein Betroffener Lösch- und Sperransprüche gegenüber dem BSI über die dort genannten wegen geltend machen.

3.3.7 Projekt

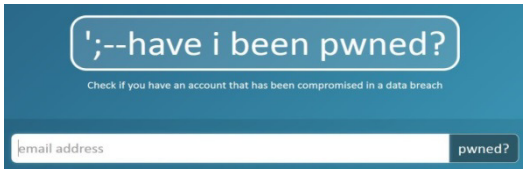
Das von Troy Hunt betriebene Projekt haveibeenpwned.com (HIBP) entstand im Nachklang des Adobe-Data-Breaches.[138] Dem Entwickler und Betreiber fiel im Rahmen der Schadensanalyse auf, dass kompromittierte Nutzerkonten aus einem Breach immer wieder auftauchten. Um den betroffenen Nutzern eine Möglichkeit einzuräumen überhaupt davon Kenntnis zu erlangen, wurde die Webseite mit einer Suchfunktion für E-Mail-Adressen und Benutzernamen eingerichtet.

[137] https://www.sicherheitstest.bsi.de/
[138] Hunt: Who, what & why, über: https://haveibeenpwned.com/About (abgerufen am 03.08.2018).

Sachverhalt

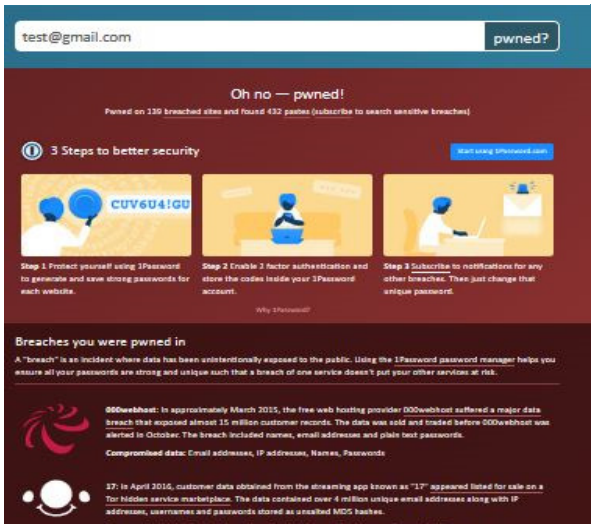
Im Hintergrund wird im Durchschnitt alle 40 Sekunden ein neuer Data Breach zur bestehenden Datenbank hinzugefügt. Jede Indexierung ist – wenn möglich – mit einer kurzen Beschreibung des Vorfalls sowie Angaben zum Datum des Vorfalls und der Indexierung, Anzahl der Betroffenen (Konten) und betroffene Datenkategorien versehen.

Abb. 8 Suchanfrage



Der Nutzer hat drei Möglichkeiten E-Mail-Adressen zu überprüfen. Eine E-Mail-Adresse kann überprüft werden indem der Nutzer diese über das Eingabefeld eingibt (Abb. 8)[139]. Daraufhin erhält der Nutzer direkt eine Rückmeldung ob und wenn ja in welchen Data Breaches (aus der HIBP-Datenbank) diese Adresse gefunden wurde (Abb. 9)[140]. Eine zweite Möglichkeit ist die Benachrichtigung nach Voranmeldung. Hierbei kann der Nutzer seine E-Mail-Adresse dauerhaft hinterlegen und wird per E-Mail benachrichtigt, sobald ein Vorfall die entsprechende Adresse enthält. Über diesen Weg kann der Nutzer außerdem besonders sensible Vorfälle einsehen. Diese speziellen Breaches sind nicht öffentlich durchsuchbar.

Abb. 9 oh no - pwned



Eine Dritte Möglichkeit ist die Suche nach allen E-Mail-Adressen zu einer Domain. Diese Suche ist nur für Nutzer möglich, die nachweislich die Kontrolle über die Domain bzw. die Website ausüben, wie beispielsweise Administratoren. Eine „domain search“ liefert alle betroffenen E-Mail-Adressen zu der angegebenen Domain. Abhängig von der getroffenen

[139] https://haveibeenpwned.com/ (abgerufen am 30.07.2018).
[140] Screenshot: Ergebnis einer Testeingabe: https://haveibeenpwned.com/ (abgerufen am 30.07.2018).

Auswahl können nur die bereits bekannten Leaks durchsucht oder auch die Warnfunktion für neue Data Breaches gemeldet werden.[141]

Die Passwortsuche gestattet dem Nutzer zu überprüfen ob ein von ihm verwendetes Passwort bereits in einem Breach vorkommt unabhängig von der E-Mail-Adresse.

Dies dient vor allem dazu Angriffe mit Hilfe von *rainbow tables* zu erschweren. Passwörter, die bereits in Data Breaches vorkamen, sind insbesondere dann weniger sicher, wenn sowohl Hashwert als auch Klartext bekannt sind, da auf diese Weise nicht mehr, wie bei *brute force-Angriffen* alle Möglichkeiten ausprobiert werden, sondern einfach die schon berechneten Passwörter genutzt werden können. Da im beschriebenen Verfahren nur anonymisierte Datenverarbeitet werden, wird diese Funktion hier nicht weiter untersucht.

Da alle Data Breaches, die HIBP indexiert hat und die einem Verantwortlichen zugeordnet werden konnten, in einer Übersicht zusammengestellt sind, kann der Nutzer anhand der Liste auch nachvollziehen, ob das Risiko eines Missbrauchs besteht, wenn keine personenbezogenen Daten über die Webseite eingegeben werden (Passivsuche).

Schlussfolgerungen

Verfügbarkeit

Ist eine E-Mail-Adresse in einem Leak enthalten, bekommt der Nutzer je nach Suchmethode direkt oder per E-Mail Informationen zum Breach. Solange nicht sichergestellt ist, dass die Informationen nicht mehr öffentlich verfügbar sind bleibt der Breach in der Datenbank indexiert und kann vom Nutzer abgerufen werden.

Sowohl in der öffentlichen Liste als auch in der Benachrichtigungs-Mail sind zusätzliche Informationen zu Datenkategorien, Umfang und Alter des Leaks enthalten. Bei Veröffentlichungen mittels sogenannter „Pastes“ ist in der Warn-E-Mail auch der Link zum Paste enthalten.[142]

Inhalte der Datenbank werden in der Regel nicht gelöscht. Als besonders sensibel eingestufte Links können jedoch nicht mit Hilfe der Suchfunktion durchsucht werden. Möchte der Nutzer wissen, ob eine E-Mail-Adresse in einem so klassifizierten Breach enthalten ist, ist dies über die Benachrichtigungsfunktion[143] möglich oder indirekt, indem der Nutzer die Liste[144] nach genutzten Diensten durchsucht.

---

[141] Hunt: Domain Search, über: https://haveibeenpwned.com/DomainSearch (abgerufen am 03.08.2018).
[142] https://www.troyhunt.com/watching-have-i-been-pwned-pastebin/ (abgerufen am 03.08.2018).
[143] https://haveibeenpwned.com/NotifyMe (abgerufen am 03.08.2018).
[144] https://haveibeenpwned.com/PwnedWebsites (abgerufen am 03.08.2018).

Grundsätzlich ist die Verfügbarkeit der Informationen von der Zugriffsmöglichkeit des Betreibers abhängig. Da dieser aus gutem Grund keine Leaks ankauft, kann es durchaus zu Verzögerungen kommen bis ein Leak in die Datenbank aufgenommen werden kann.

Vertraulichkeit

Das größte Problem der Suche nach betroffenen E-Mail-Adressen über HIBP ist die fehlende Authentifizierung des Nutzers. Jeder kann jede beliebige E-Mail-Adresse überprüfen und erhält Auskunft darüber ob diese von einem Data Breach betroffen war und damit auch bei welchen Diensten sich mit dieser Adresse angemeldet wurde. Zwar sind die - nach Ermessen des Betreibers - besonders sensiblen Breaches nicht öffentlich durchsuchbar. Diese machen mit derzeit 21 Leaks von über 80.000 Pastes aber nur einen verschwindend geringen Anteil aus.[145] Die Wertung ist etwas einseitig, denn die entsprechenden Seiten beschränken sich auf einen sexuellen Kontext. Es sind jedoch auch andere Konstellationen denkbar, die sich nachteilig auf den Betroffenen auswirken können, beispielsweise wenn eine E-Mail-Adresse mit Seiten in Verbindung gebracht wird, die die Legalisierung von Cannabis thematisieren, nach europäischem Datenschutzrecht besonders sensible Daten gemäß Art. 9 Abs. 1 DSGVO enthalten oder Kinder betreffen[146]. Zu Analysezwecken werden Hinweise auf konkrete Leaks vom Betreiber ausgewertet. Hierzu hat dieser Zugriff auf alle darin enthaltenen personenbezogenen Daten.

Abfragen sind begrenzt auf eine Anfrage alle 1,5 Sekunden pro IP-Adresse.[147] Hiermit wird eine automatisierte, systematische Suche nach kompromittierten E-Mail-Adressen erschwert. Die Schnittstelle ist zudem nur über eine transportverschlüsselte Verbindung erreichbar.

Integrität

Das Alter der Leaks ist in den Informationen zum Data Breach mit enthalten. Die Integrität der Daten im engeren Sinne (Echtheit/Richtigkeit) wird in der Regel anhand von fünf Kriterien bestimmt. Hinweise auf einen tatsächlichen und neuen Vorfall sind eine öffentliche Bekanntmachung des betroffenen Dienstes, ein negatives Suchergebnis bei Google, die Datenstruktur der Dateien entspricht der eines Breaches, die Angreifer haben ihren Angriff plausibel geschildert und die Reputation der Angreifer lässt auf eine echten Data Breach schließen.[148]

---

[145] Hunt: What is a „sensitive breach“?, über: https://haveibeenpwned.com/FAQs (abgerufen am 03.08.2018).
[146] Siehe VTech-Data Breach, über: https://www.troyhunt.com/when-children-are-breached-inside/ (abgerufen am 03.08.2018).
[147] Rate limiting, über: https://haveibeenpwned.com/API/v2 (abgerufen am 03.08.2018).
[148] Hunt: How is a breach verified as legitimate?, über: https://haveibeenpwned.com/FAQs (abgerufen am 03.08.2018).

Kann ein Breach nicht verifiziert werden, wird er dennoch in die Datenbank aufgenommen. Hintergrund ist, dass trotz berechtigter Zweifel an der Echtheit der Daten oder der Quelle personenbezogene Daten enthalten sind, die dem Betroffenen nicht vorenthalten werden sollen. Diese Einträge werden jedoch als nicht-verifiziert („unverified“) bzw. als fingiert („fabricated“) gekennzeichnet.[149]

Für den unwahrscheinlichen Fall, dass Daten aus einem Breach nicht mehr verfügbar sind, wird ein Eintrag als ruhend („retired“) klassifiziert.[150]

Einen Anspruch auf Vollständigkeit kann auch dieser Dienst nicht erheben, denn Leaks die nicht veröffentlicht wurden und Breaches die nicht erkannt worden sind, sind nicht in der Datenbank enthalten.[151]

Verkettung

In diesem Zusammenhang ist vor allem die Abfrage kompletter Domains problematisch. Prinzipiell kann jeder E-Mail-Provider eine solche Suchanfrage stellen und damit in Erfahrung bringen welche Nutzer/Kunden/Arbeitnehmer von welchen Leak betroffen sind. Hier besteht entsprechend das Risiko einer umfassenden Kenntnis über die Aktivitäten der E-Mail-Adressnutzer, ohne dass die Betroffenen hiervon zwingend in Kenntnis gesetzt werden.

Intervenierbarkeit

Der Inhaber einer E-Mail-Adresse kann diese für die öffentliche Suche sperren lassen (Opt-out). Dies ist eine Möglichkeit einen Missbrauch durch Dritte zu verhindern. Allerdings ist der Prozess nicht umkehrbar und muss durch beantworten einer Verifikationsmail bestätigt werden. Die Benachrichtigung nach Voranmeldung ist jedoch weiterhin möglich.

Auch die Domain Search erfordert eine Bestätigung darüber, dass der Nutzer hierzu authentisiert ist.[152]

Transparenz

Auf der Webseite haveibeenpwned.com ist ausführlich beschrieben wie der Service arbeitet und wie personenbezogene Daten verarbeitet werden bzw. wie mit den Daten aus den Breaches umgegangen wird.

---

[149] Hunt: What is an „unverified“ breach?; What is a „fabricated“ breach?, über: https://haveibeenpwned.com/FAQs (abgerufen am 03.08.2018).
[150] Hunt: What is a „retired“ breach?, über: https://haveibeenpwned.com/FAQs (abgerufen am 03.08.2018).
[151] Hunt: My email was not found – does that mean i haven’t bee pwned?, über: https://haveibeenpwned.com/FAQs (abgerufen am 03.08.2018).
[152] Hunt: When you search for a domain, über: https://haveibeenpwned.com/Privacy (abgerufen am 03.08.2018).

Die API steht im Rahmen der Creative Commens-Lizenz (Version 4.0) zur freien Verfügung unter der Bedingung, dass die Datenquelle genannt wird (CC BY 4.0).[153]

Es fehlt ein Hinweis darauf, was mit den Daten aus den Leaks sonst noch passiert. Zwar sind im Online-Dienst keine weiteren als die beschriebenen Daten enthalten, die Blog-Einträge des Betreiber zeigen jedoch eindeutig, dass dieser Zugriff auf sämtliche Informationen eines Leaks hat. Es wäre daher im Interesse aller Betroffenen zu klären ob diese Originaldaten (wenn auch offline) alle gespeichert bleiben, wie und was genau gespeichert wird, ob die Daten für andere Zwecke genutzt und möglicherweise an Dritte übermittelt werden bzw. wer Zugriffsrechte hat und wie lange alles gespeichert bleibt. Im privaten Blog von Troy Hunt heißt es hierzu nur: „I lock it away out of easy reach (for obvious reasons)".[154]

Gegenmaßnahmen

Das BSI rät im Falle eines Identitätsdiebstahls dazu Mahnungen, die per E-Mail eintreffen, zu löschen, Passwörter zu ändern sowie sich mit Dienstleistern in Verbindung zu setzen, zu deren Konten Daten „abhandengekommen" sind, z.B. Banken oder soziale Netzwerke.[155] In jeweils einem Nebensatz erwähnt das BSI zudem das der Betroffene Anzeige bei der Polizei erstatten und ggf. einen Anwalt konsultieren soll. Auch die Rekapitulation einer solchen Erfahrung regt das BSI an und zielt damit eher auf die Vermeidung neuer Schäden als die Beseitigung bereits vorhandener ab.

Statt den durch einen Datenmissbrauch entstandenen Schaden zu beseitigen, können und sollten die Nutzer selbst Präventionsmaßnahmen ergreifen um dies zu verhindern. Sowohl das Bundeskriminalamt (BKA) wie auch das BSI

3.4 Fazit

In der Gesamtbetrachtung gibt es bei jedem Identitätsschutz-Modell Verbesserungsmöglichkeiten. Es gibt jedoch zwischen den Produkten gravierende Unterschiede in Bezug auf die Umsetzung der im Datenschutz relevanten Gewährleistungsziele (siehe Abschnitt 3.2).

Für den Nutzer der untersuchten Identitätsschutz-Modelle stellt die Verfügbarkeit der Suchergebnisse ein entscheidendes Erfolgskriterium dar. Die Häufigkeit mit der nach sensiblen Daten gesucht werden kann, ist von Anbieter zu Anbieter sehr verschieden. Während die kontenbasierten Dienstleister regelmäßig und engmaschig suchen, entscheidet bei den verdachtsabhängigen Dienstleistern der Nutzer selbst, wann und wie oft gesucht werden soll.

---

[153] Lizenzinformationen, über: https://haveibeenpwned.com/API/v2 (abgerufen am 03.08.2018).
[154] Hunt: No, I cannot share data breaches with you, über: https://www.troyhunt.com/no-i-cannot-share-data-breaches-with-you/ (abgerufen am 03.08.2018).
[155] BSI: Identitätsdiebstahl – Hilfe für Betroffene, über: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Hilfe/Hilfe_Betroffene.html (zuletzt abgerufen am 28.06.18).

Grundsätzlich kann der Nutzer hier über die Produktauswahl selbst entscheiden, welche Taktung als angemessen empfunden wird. Neben der subjektiven Einschätzung des Nutzers ist jedoch auch objektiv zu beurteilen in welcher Frequenz eine Suche erforderlich ist. Eine Möglichkeit die Intervenierbarkeit für den Nutzer zu erhöhen, wäre diesen die Intervalle selbst einstellen zu lassen.

Die untersuchten Identitätsschutzmodelle überlassen zudem die Risikobeurteilung der subjektiven Einschätzung ihrer Nutzer oder sie nehmen eine Beurteilung vor, offenbaren jedoch nicht aufgrund welcher Kriterien die jeweilige Einschätzung zustande gekommen ist. Dies entspricht nicht der Intention des Gesetzgebers. Besser wäre es jedoch eine Risikobeurteilung vorzunehmen, der objektive Kriterien zu Grunde gelegt werden. Sofern in den vorliegenden Modellen von Seiten des Anbieters überhaupt eine Risikoeinteilung erfolgt, ist diese nicht transparent gestaltet. Der Nutzer kann nicht nachvollziehen, welche Kriterien in die Risikobewertung einfließen. Dies verleitet tendenziell dazu, dass zu viele Angaben gemacht werden und der Nutzer nicht zwischen verschiedenen Risikostufen differenziert. Insbesondere personenbezogene Daten oder Konstellationen, die nur ein geringes Risiko für den Betroffenen mit sich bringen, rechtfertigen unter den Gesichtspunkten der Verhältnismäßigkeit keine lückenlose Überwachung aller digitalen Identitäten. In diesem Zusammenhang sind beispielsweise Kommunikationsdaten, wie E-Mail-Adressen oder Telefonnummern zu sehen. Bei einer Suche 24 Stunden am Tag erfolgt eine Dauerüberwachung der Daten, die der Nutzer zur Verfügung gestellt hat. Dass dies bei risikoarmen Daten tatsächlich notwendig ist, kann bezweifelt werden. Ein ständiges Alarmschlagen führt zudem zur Abstumpfung der Betroffenen und der eigentliche Zweck der Warnung, den Betroffenen zum Ergreifen von Gegenmaßnahmen zu veranlassen, verpufft.

Werden neben der Suchfrequenz, die Art der Suche und die Quellen in Betrachtung gezogen, ergeben sich daraus weitere Risiken für den Betroffenen. Die Ergebnisse einer Onlinesuche können von Tag zu Tag variieren. Die volatile Natur des Internets kann dazu führen, dass Fundstellen von heute auf morgen auftauchen und wieder verschwinden. Insofern ist es verständlich, dass die Anbieter auf eine engmaschige Suche setzen. Insbesondere bei den kontenbasierten Schutzmodellen ist jedoch nicht klar wie genau die Suche abläuft. Da das Verfahren an sich intransparent ist, ist auch keine Aussage zum Schutzniveau das der Anbieter bietet möglich.

Owl Detect, HPI, HIBP und das BSI halten im Gegensatz dazu eine eigene Datenbank vor und gleichen alle Daten der Kunden nur gegen diese Datenbestände ab. Der Vorteil dieser Methode ist, dass hierbei keine Suchbegriffe bzw. Nutzerdaten ins Netz gelangen. Ein weiterer Vorteil besteht darin, dass die Daten pseudonymisiert und verschlüsselt vorgehalten werden können. Der Datenbankabgleich erhöht somit die Vertraulichkeit der Suchparameter. Hier ist das gebotene Schutzniveau entsprechend höher.

Eine Cleanerfunktion, wie sie von IDPROTECT oder meineSCHUFA angeboten wird, ist damit jedoch nicht möglich. Dieser Service beinhaltet jedoch keine juristische Prüfung des Anspruchs. Es ist also fraglich, wie sinnvoll diese Funktion tatsächlich ist, wenn das gewünschte Ergebnis gar nicht erreicht werden kann.

Bis auf den BSI-Sicherheitstest sind alle Angebote darauf ausgelegt ihren Datenbestand stetig zu erweitern. Die Speicherdauer während der Nutzung ist nicht begrenzt. Die Speicherfristen über die Nutzung hinaus sind nicht in allen Fällen festgelegt oder eindeutig. Präventiv erhobene Daten werden ebenfalls sehr lange vorgehalten. Insgesamt fehlt es an automatisierten Löschroutinen und damit an einer konsequenten Umsetzungen der Datenminimierung.

Angaben zu den Fundstellen geben die Anbieter nur teilweise bekannt. Lediglich beim BSI sind die genauen Hintergründe bekannt. Die Angebote mit Cleaner-Funktion geben die zu bereinigenden Fundstellen ebenfalls bekannt. Hierbei handelt es sich jedoch um Informationen, die der Nutzer mittels Suchmaschine auch selbst recherchieren könnte. Die fehlende Angabe der Fundstellen kann durchaus im Sinne des Nutzers sein, z.B. damit dieser nicht unbedarft auf den entsprechenden Seiten „herumsurft". Die zivilrechtliche Verfolgung von Ansprüchen wird dadurch jedoch erschwert, denn hier liegt die Beweislast beim Betroffenen. Keines der Produkte sieht eine tatsächliche Unterstützung der Betroffenen nach der Benachrichtigung vor. Die zur Verfügung gestellten Informationen sind allgemein gehalten und nicht auf den Individuellen Datenschutzvorfall angepasst. Die vom Betroffenen auf dieser Grundlage getroffenen Maßnahmen helfen unter Umständen gar nicht das entstandene Risiko zu mindern oder Schäden zu vermeiden.

Die Benachrichtigung bei allen Anbietern erfolgt mittels unverschlüsselter E-Mail-Kommunikation. In keinem Fall gab es eine Option zur Eröffnung eines sicheren Kommunikationskanals. Die Anbieter bei denen ein Nutzerkonto angelegt wird, hätten erstens die Möglichkeit einen eigenen Kommunikationsweg bereitzustellen, zweitens könnten sie dem Kunden ermöglichen bspw. einen öffentlichen PGP-Schlüssel zu übermitteln um auf diese Weise Berichte und Meldungen verschlüsselt zu übermitteln. Teilweise ist zumindest ein zweiter Kanal möglich. Dies ist vor allem für die Fälle relevant, in denen die Zugangsdaten zum E-Mail-Konto veröffentlicht wurden und nicht gewährleistet werden kann, dass der Inhaber des E-Mail-Kontos noch die Kontrolle über das Postfach hat. Auch in diesem Fall wäre eine Ende-zu-Ende-verschlüsselte Kommunikation sinnvoll. Besonders kritisch ist in diesem Zusammenhang das HIBP-Projekt zu sehen. Hier werden alle Leaks in denen eine E-Mail-Adresse enthalten war direkt auf der Webseite angezeigt. Damit kann jeder Besucher der Webseite jede beliebige E-Mail-Adresse „testen". Diese Abfrageform ist mit den Anforderungen des europäischen Datenschutzrechts nicht vereinbar.

Vertraulichkeit ist nicht nur im Rahmen der Kommunikation sondern auch im Umgang der Anbieter mit den zur Verfügung gestellten Daten und den daraus gewonnenen Erkenntnis-

sen zu gewährleisten. Eine 2-Faktor-Authentifizierung verwendet nur meineSCHUFA. Hier wird mittels Post-Ident-Verfahren sichergestellt, dass der Nutzer des Dienstes tatsächlich Inhaber der (digitalen) Identität ist. IDPROTECT stellt die Zugangsdaten nur auf Basis einer Versicherungspolice zur Verfügung, prüft jedoch in der Folge nicht ob die gesuchten Daten mit den Daten des Versicherungsnehmers übereinstimmen. Dem Risiko, dass personenbezogene Daten Dritter durch den Nutzer ausgespäht werden, wurde lediglich durch eine Klausel in den AGB begegnet. Die Wirksamkeit dieser Maßnahme kann bezweifelt werden, zumal bei dieser Variante auch zusätzliche Konten möglich sind für die überhaupt keine Verifikation sondern nur einen funktionierende E-Mail-Adresse der Nutzer erforderlich ist. Der Schutz personenbezogener Daten Dritter ist – außer beim HPI-Leak Checker und beim BSI-Sicherheitstest – bei allen Anbietern ein Problem, da die Verifikation der Einzelangaben einen hohen Aufwand erfordern würde. Dies darf jedoch nicht zu Lasten Dritter gehen.

Grundsätzlich ist das Verkettungspotential bei kontenbasierten Angeboten deutlich größer, da hier z.T. sehr umfangreiche Angaben möglich sind. Das Risiko der Verarbeitung für den Betroffenen ist entsprechend hoch. Aber auch die auf Einzelabfragen basierenden Systeme können über die E-Mail-Adresse Informationen aus mehreren Leaks zu einem Profil verketten. Auch hier sind IDPROTECT und meineSCHUFA zu kritisieren, da diese sich vorbehalten personenbezogenen Daten auf Grund berechtigter Interessen zu verarbeiten. Da es keine Differenzierung zwischen den Leak-Checkern und anderen Produkten der beiden Anbieter gibt, ist nicht ersichtlich inwieweit Daten weiterverwendet werden. Es ist nicht bekannt ob die Bestehenden Verfahren einer Vorabkontrolle unterzogen wurden. Einer Datenschutz-Folgenabschätzung, wie sie Art. 35 DSGVO für besonders risikoreiche Verfahren vorsieht, wurde wahrscheinlich nicht durchgeführt, denn hierbei hätten zumindest die größten Probleme der Verfahren auffallen müssen. Problematisch sind auch die meist fehlenden oder unpräzisen Angaben zur Weitergabe, Speicherdauer und zum Speicherort. So handelt es sich bei der Affinion GmbH um eine Tochter eines global agierenden Unternehmens und der technische Dienstleister von CPP (Owl Detect) sitzt in Großbritannien, was ab März 2019 mit dem Austritt aus der EU zum Problem werden könnte, da es sich hierbei unter Umständen um einen Drittstaat ohne Angemessenheitsbeschluss gemäß Art. 45 DSGVO handelt. Andererseits ist CSID seit 2016 Teil von Experian.[156] Experian ist eine weltweit agierende Auskunftei. Die Weitergabe personenbezogener Daten bei der Übernahme oder Eingliederung von Firmen in andere Unternehmen ist spätestens seit dem Kauf von WhatsApp durch Facebook als datenschutzrechtliches Problem bekannt.[157] Für den Betroffenen ist es auf Grund der Verflechtungen unmöglich nachzuvollziehen, wo seine Daten gespeichert werden,

[156] Owl: FAQ – Wie sicher sind meine persönlichen Daten, die ich an Owl übermittle?, über: https://www.owldetect.de/faqs/ (am 21.11.2018); CSID: https://www.csid.com/company/ ; Experian: https://www.experianpartnersolutions.com/company/ ;

[157] DPA: WhatsApp darf weiterhin Datendeutscher Nutzer nicht an Facebook weiterleiten, über: https://www.heise.de/newsticker/meldung/WhatsApp-darf-weiterhin-Daten-deutscher-Nutzer-nicht-an-Facebook-weiterleiten-3984432.html (21.11.2018).

welche Unternehmensteile Zugriff haben und an wen möglicherweise Datenübermittelt werden.

Für den Endnutzer mag sich dies schlussendlich in der Frage auskristallisieren, welchem Anbieter das meiste Vertrauen entgegen gebracht wird. Die Stichprobe hat gezeigt, dass das Hauptgeschäftsfeld eines Anbieters Einfluss auf die Gestaltung der Verarbeitung hat. Auch, wenn einige der Angebote sich auf den ersten Blick ähneln, spielt die grundlegende Motivation, die dahinter steht für die Bewertung aus Datenschutzsicht eine entscheidende Rolle. Ein Anbieter dessen Haupttätigkeit im Bereich IT-Sicherheit liegt, wird seine Reputation nicht durch eine Zweckdehnung gefährden. Andere Anbieter, die Identitätsschutz-Werkzeuge im Rahmen von Kundenbindungsprogrammen zu Marketingzwecken einbinden, generieren einen wirtschaftlichen Mehrwert hingegen erst durch die zusätzlichen Informationen, die hierdurch direkt oder indirekt zur Verfügung stehen. Dies spiegelt sich auch in der Implementierung der Werkzeuge wieder. Die oben genannten Beispiele der Versicherung und Auskunftei sind in Bezug auf Informationen und Transparenz mangelhaft sowie in Bezug auf den Schutz personenbezogener Daten Dritter teilweise ungenügend. Die Art und Weise der Umsetzung im Vergleich zu den anderen Anbietern ist ein Indiz dafür, dass der angepriesene Identitätsschutz hauptsächlich der Marketingstrategie des Unternehmens und nicht dem Datenschutz der Kunden dient.

Aufgrund der umfangreichen Datenverarbeitung, der Vielzahl von Betroffenen, den Verkettungsmöglichkeiten (inklusive der Möglichkeit zur Profilbildung) und verarbeiteten Datenkategorien und des insgesamt hohen Risikos der Datenverarbeitung sollten alle Anbieter ihre Verarbeitung auf DSGVO-Konformität überprüfen. Keines der untersuchten Modelle konnte unter den Kriterien des Datenschutzes als vorbehaltlos einsetzbar überzeugen.

4 Empfehlungen für EIDI

Nachdem die Analyse die Schwachstellen bestehender Identitätsschutz-Modelle offenbart hat, sollen die Anforderungen für das EIDI-Framework hieraus abgeleitet werden.

Nicht alle Daten taugen für einen Identitätsdiebstahl. Es ist eine Differenzierung zwischen verschiedenen Angriffsszenarien erforderlich, da verschiedene Kombination personenbezogener Daten einen Identitätsdiebstahl unterschiedlich wahrscheinlich machen.

Das Risikopotential verschiedener Kombinationen sollte im Vorfeld anhand objektiver Kriterien festgelegt werden. Eine unrechtmäßig veröffentlichte E-Mail-Adresse oder Telefonnummer stellt zwar einen Datenschutzvorfall und damit einen Verstoß gegen das Daten-

schutzrecht dar. Diese Informationen allein eignen sich jedoch nicht für einen Identitätsdiebstahl. Die Risikoanalyse sollte dies berücksichtigen und auch dem Betroffenen in der Benachrichtigung vermitteln. Ziel sollte es sein dem Betroffenen eine realistische Einschätzung der Situation zu ermöglichen. Dieser sollte in die Lage versetzt werden mögliche Schäden zu antizipieren um zielgerichtete und wirkungsvolle Präventionsmaßnahmen ergreifen zu können. Die Festlegung auf bestimmte Datenkategorien ermöglicht zudem die nicht erforderlichen Daten zu löschen und fördert damit die Datenminimierung.

Das EIDI-Framework sollte zudem spezifizieren, unterwelchen Umständen welche Art von Risiko besteht und dies auch nach außen kommunizieren. Dieser Aspekt der Transparenz kann langfristig helfen die Sensibilität für Datenschutzvorfälle zu erhöhen. Die Sensibilität der Betroffenen ist wiederum die Voraussetzung für eine angemessene Reaktion und die Einleitung sowie Umsetzung notwendiger Maßnahmen nach einem Datenschutzvorfall. Grundsätzlich sind Transparenzanforderungen in drei Bereichen zu erfüllen: a) Im Rahmen der Dokumentation und Präsentation des Verfahrens (Verarbeitungsverzeichnis, DSFA, Webseite), b) im Zuge der Informationspflichten beim ersten Kontakt mit dem Betroffenen und c) bei der eigentlichen Inhalt der Warnung. Die Transparenzanforderungen sind von allen beteiligten Akteuren zu erfüllen.

Integrität, Vertraulichkeit und Verfügbarkeit sind entsprechend des Stands der Technik und nach Maßgabe datenschutzrechtlicher Vorschriften und IT-Sicherheitsstandards über den gesamten Lebenszyklus der Verarbeitung und des Verfahrens hinweg zu gewährleisten. Darüber hinaus sind verschiedene Kommunikationskanäle in Betracht zu ziehen, die eine höhere Vertraulichkeit der Nachrichtenübermittlung gewährleisten als E-Mails und SMS.

Dem hohen Verkettungspotential sind besondere Schutzmaßnahmen entgegenzusetzen. Die Spiegelung der im Internet frei kursierenden Identitätsdaten darf einen weiteren Datenmissbrauch nicht begünstigen, zumal es sich hierbei um eine Zentralisierung der vorhandenen Leaks an einer einzigen Stelle handelt. Verknüpfungen zwischen Daten, Datensätzen bzw. vollständigen Leaks sowie zwischen System und Prozessen sind einer strengen Erforderlichkeitsprüfung zu unterziehen. Dies gilt auch im Hinblick auf die Weiterverwertung zu Forschungszwecken. Es sind die spezifischen Forschungszwecke und die geforderten geeigneten Garantien zum Schutz der personenbezogenen Daten gemäß Art. 89 Abs. 1 DSGVO festzulegen.

Die Forschung in diesem Bereich kann einerseits helfen die Aufklärungsquote bei Cyberkriminalität zu erhöhen. Andererseits könnte der Zeitraum bis zur Entdeckung eines Datenlecks bei einem Verantwortlichen verkürzt werden. Die schnellere Kenntnis eines Lecks kann unter Umständen die Zahl der Betroffenen minimieren sowie zur früheren Ergreifung von Gegen- und Schutzmaßnahmen führen. Die Identifikation der Quellen eines Datenlecks

erhöht zudem den Druck auf verantwortliche Stellen Vorfälle tatsächlich zu melden und nicht zu verschleiern.

Dem von den bestehenden Systemen vernachlässigte Teil der Nachbetreuung – also ab dem Zeitpunkt des Empfangs der Warnung – sollte wesentlich mehr Aufmerksamkeit gewidmet werden. Ein Konzept zum Umgang mit Datenschutzvorfällen sollte den Betroffenen in die Lage versetzen sich vor negativen Auswirkungen zu schützen. Insbesondere nach einem Identitätsdiebstahl sind die Betroffenen häufig über Jahre mit den Nachwirkungen belastet.[158] Zudem ist eine umfassende Aufklärung der Betroffenen über die möglichen Folgen eines Datenmissbrauchs erforderlich, auch wenn es (noch) nicht zu einem Identitätsdiebstahl gekommen ist.

Wünschenswert wäre ein Ansatz der dazu führt, dass der Betroffene ab einem bestimmten Zeitpunkt nicht mehr mit dem Identitätsdiebstahl konfrontiert wird. Hier ist ein völlig neues Konzept erforderlich, dass die Lebensdauer digitaler Identitäten berücksichtigt. Außerdem sollten Opfer von Cyber-Kriminalität Anzeige erstatten[159] und wenn möglich auch bei der Durchsetzung zivilrechtlicher Ansprüche unterstützt werden.

[158] http://identitaetsdiebstahl.info/index.php/der-fall-von-tina-groll/ (22.11.2018).
[159] Bundeskriminalamt: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html (22.11.2018).

5 Abbildungsverzeichnis

6 Literaturverzeichnis

AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.): Das Standard-Datenschutzmodell (V 1.1), Düsseldorf 2018.

Albrecht/ Jotzo: Das neue Datenschutzrecht der EU, 1. Aufl., Baden-Baden 2017.

Cooley(1956): *The Two Major Works of Charles H. Cooley: "Social Organization" [1909] – "Human Nature and the Social Order" [1902]*; introd. by Robert Cooley Angell, Glencoe, Illinois: The Free Press; S. 168-210.

DSK: Kurzpapiere Nr. 1-19 (Stand August 2018), über: https://www.datenschutzzentrum.de/dsgvo/#kurzpapiere

Erikson (1979 [1959]): *Identität und Lebenszyklus*, Frankfurt am Main: Suhrkamp.

Gonscherowski, Hansen, Rost: Resilienz – Eine neue Anforderung aus der Datenschutz-Grundverordnung, in: DuD, 7/2018, S. 442-446.

Otfried Höffe (Hrsg): Aristoteles - Politik, 2. Aufl. (2011), Akademie Verlag.

Koops/ Leenes: Identity Theft, Identity Fraud and/or Identity-related Crime, in: Datenschutz und Datensicherheit, 9/2006 (30. Jg), S. 553-556.

Mead(1968 [1934]): *Geist, Identität und Gesellschaft*, Frankfurt am Main: Suhrkamp. Im Original: (1934): Mind, Self, and Society, Chicago: The University of Chicago Press.

Leeb/ Liebhaber: Grundlagen des Datenschutzrechts, in: Juristische Schulung 2018, S. 534-538.

Lersch: Der Mensch als soziales Wesen. Eine Einführung in die Sozialpsychologie, 2. Aufl. 2013.

Locke(1981 [1690]): *Versuch über den menschlichen Verstand*, Band 1, Hamburg: Felix Meiner Verlag.

Paal/ Pauly: Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Storch: Identität in der Postmoderne–mögliche Fragen und mögliche Antworten, in: Allgemeine Heilpädagogik. Eine interdisziplinäre Einführung, 1999, 2. Jg., S. 70-84.

AK Technik: Arbeitskreis Tecnik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK): Das Standard-Datenschutzmodell (V 1.1), Düsseldorf 2018, online: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

Albrecht/ Jotzo: Das neue Datenschutzrecht der EU, 1. Aufl., Baden-Baden 2017.

Cooley, C. H. (1956): The Two Major Works of Charles H. Cooley: "Social Organization" [1909] – "Human Nature and the Social Order" [1902]; introd. By Robert Cooley Angell, Glencoe, Illinois: The Free Press; S. 168-210.

DSK: Kurzpapiere Nr. 1-19 (Stand August 2018), online https://www.datenschutzzentrum.de/dsgvo/#kurzpapiere

Erikson, E. H. (1979 [1959]): Identität und Lebenszyklus, Frankfurt am Main: Suhrkamp.

Gonscherowski, Hansen, Rost: Resilienz – Eine neue Anforderung aus der Datenschutz-Grundverordnung, in: DuD, 7/2018, S. 442-446.

Höffe (Hrsg): Aristoteles - Politik, 2. Aufl. (2011), Akademie Verlag.

Koops / Leenes: Identity Theft, Identity Fraud and/or Identity-related Crime, in: Datenschutz und Datensicherheit, 9/2006 (30. Jg), S. 553-556, über: http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf.

Mead (1968 [1934]): Geist, Identität und Gesellschaft, Frankfurt am Main: Suhrkamp. Im Original: (1934): Mind, Self, and Society, Chicago: The University of Chicago Press.

Leeb/ Liebhaber: Grundlagen des Datenschutzrechts, in: Juristische Schulung 2018, S. 534-538.

Leenes: ID-related Crime: Towards a Common Ground for Interdisciplinary Research (D5.2b), über: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf (abgerufen am 10.07.2018), 59 f.

Lersch: Der Mensch als soziales Wesen. Eine Einführung in die Sozialpsychologie, 2. Aufl. 2013.

Locke (1981 [1690]): Versuch über den menschlichen Verstand, Band 1, Hamburg: Felix Meiner Verlag.

Paal/ Pauly: Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., München 2018.

Storch: Identität in der Postmoderne–mögliche Fragen und mögliche Antworten, in: Allgemeine Heilpädagogik. Eine interdisziplinäre Einführung, 1999, 2. Jg., S. 70-84.