Usability trifft DSGVO: Wie gehe ich mit sensiblen Daten um?

Workshop des German UPA-Arbeitskreises Usable Security & Privacy

Hartmut Schmitt
HK Business Solutions GmbH
Sulzbach, Germany
hartmut.schmitt@hk-bs.de

Mandy Balthasar
Universität der Bundeswehr München, Germany
mandy.balthasar@unibw.de

Timo Jakobi
Universität Siegen
Siegen, Germany
timo.jakobi@uni-siegen.de

ZUSAMMENFASSUNG

Spätestens mit der Geltung der EU-Datenschutzgrundverordnung (DSGVO) sind die Themen Datenschutz und Umgang mit personenenbezogenen Daten im Berufsalltag vieler Usability Professionals angelangt. Im Workshop wird ein Ansatz vorgestellt, um personenbezogene Daten – z. B. Benutzerprofildaten wie Google Takeout oder Daten aus dem Internet of Things (kurz: IoT) aus den Bereichen Smart Metering, Smart Home oder Smart Car – in einem Dashboard aufzubereiten, zu visualisieren und dadurch verständlicher zu gestalten. Dadurch sollen Anwender und Unternehmen in die Lage versetzt werden, Entscheidungen auf einer soliden Informationsbasis treffen und souverän mit ihren (bzw. den ihnen anvertrauten) personenbezogenen Daten umgehen zu können. Gleichzeitig sollen die dahinterliegenden Prozesse aufgezeigt werden, um die Relevanz prozesszentrierter Betrachtungsweisen zu verdeutlichen, welche vor allem im IoT-Umfeld unabdingbar sind.

SCHLAGWORTE

Bedienbarkeit, Data Literacy, Datenschutz, DSGVO, Privatheit, Internet of Things, Usability, Visualisierung

1 Datenschutz im Berufsalltag der Usability- und UX-Professionals

Mit der EU-Datenschutzgrundverordnung [1] gilt seit dem 25. Mai 2018 innerhalb der Europäischen Union ein einheitliches Datenschutzrecht. Ziel der DSGVO ist es, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen, insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 DSGVO [2]). Betroffen von der DSGVO sind alle Unternehmen, welche personenbezogene Daten erfassen, verarbeiten und speichern. Diese Unternehmen stehen vor der Herausforderung, praktikable und gleichzeitig benutzerfreundliche Lösungen zu finden, um rechtskonform mit der Identität von Kunden sowie mit deren Einwilligungen zur Verarbeitung personenbezogener Daten umzugehen. Denn bei Nichteinhaltung der DSGVO-Vorschriften drohen den Unternehmen sowohl empfindliche Bußgelder als auch strafrechtliche Sanktionen. Gleichzeitig ist auch ein möglicher Reputationsschaden nicht zu unterschätzen.

Personenbezogene Daten im Sinne der DSGVO sind beispielsweise Namen und E-Mail-Adressen natürlicher Personen, aber auch Informationen, welche eine indirekte Identifizierung ermöglichen, sogenannte personenbeziehbare Daten, etwa Videoaufnahmen oder getrackte IP-Adressen. Entscheidend für die Aussagekraft einer Angabe ist hierbei nicht die technische Form, sondern deren Verwendungszusammenhang. Für Usability- und User-Experience-Professionals (UUX-Professionals) ist die DSGVO daher in zweierlei Hinsicht relevant. Zum einen erheben bzw. verarbeiten UUX-Professionals im Rahmen ihrer Arbeit oft selbst personenbezogene Daten von Kunden oder Testteilnehmern. Sie müssen daher für einen rechtskonformen Umgang mit Kundenidentitäten bzw. Einwilligungen zur Verarbeitung personenbezogener Daten sorgen. Ferner müssen sie sicherstellen, dass erhobene Daten bei Bedarf pseudonymisiert oder anonymisiert werden, um die Privatsphäre der Probanden zu schützen. Zum anderen sind UUX-Professionals maßgeblich am Design der interaktiven Systeme beteiligt, welche die DSGVO-konforme Verarbeitung personenbezogener Daten gewährleisten sollen. Hier kommen die DSGVO-Prinzipien Privacy by Design und Privacy by Default ins Spiel (Art. 25 DSGVO [3]), also die Gewährleistung von Datenschutz bzw. Datenminimierung durch eine entsprechende Ausgestaltung der Hard- und Softwarekomponenten sowie nutzerfreundliche Voreinstellungen.

2 Umsetzung der DSGVO

Vor allem im EU-Ausland werden die Regelungen der DSGVO häufig als Erfolg bewertet: „Der Zweck der DSGVO ist nicht, die Verwendung personenbezogener Daten zu beschränken. Es geht darum, die Daten auf eine kontrollierte Weise zu verwenden,

Veröffentlicht durch die Gesellschaft für Informatik e.V. und die German UPA e.V. 2019 in S. Hess & H. Fischer (Hrsg.):
Mensch und Computer 2019 – Usability Professionals, 08.-11. September 2019, Hamburg

https://doi.org/10.18420/muc2019-up-0278

damit die Gesellschaft, die Bürger und das Unternehmensumfeld zufrieden sein können [4].“ Als besonders positiv wird dabei der enorme Zuwachs an Aufmerksamkeit gesehen, welcher das Bewusstsein für die Datenschutzthematik vorangetrieben hat. So haben die Unternehmen in ihren Datenschutz investiert und viele verbessern diesen stetig weiter [4].

Doch wie weit sind die Themen DSGVO, Privacy by Design und Privacy by Default tatsächlich im Berufsalltag der UUX-Professionals angekommen? Und welche Herausforderungen und Bedarfe gibt es aus deren Sicht aktuell? Um dies zu untersuchen, hat der Arbeitskreis Usable Security & Privacy der German UPA im Rahmen der UPA-Mitgliederbefragung 2018 ein Stimmungsbild zum Thema Datenschutz und DSGVO erhoben (n = 170 [erste drei Prozentangaben] bzw. 184 [Rest]) [5]. Das Ergebnis: 57,06 % der Befragten gaben an, dass sie mehr Methodenwissen zum Thema Usable Security & Privacy benötigen, 51,76 % sahen einen besonderen Bedarf an spezialisierten Werkzeugen, wie beispielsweise Richtlinien, Pattern und Checklisten für Usable Security & Privacy.

44 % der Teilnehmer wünschten sich zudem einen integrierten Entwicklungsprozess, welcher die Bereiche UUX, Security Engineering und Privacy abdeckt. 47,28 % der Befragten bestätigten, dass ihnen eigenes Fachwissen zu IT-Security- bzw. Privacy-Themen fehlt, 39,67 % vermissten gute Best Practices und Fallbeispiele für diesen Bereich. Was die konkrete Umsetzbarkeit der DSGVO angeht, herrscht bei den Usability Professionals aktuell noch eine große Unsicherheit (sehr hohe Unsicherheit: 5,43 %; hohe Unsicherheit: 36,96 %; etwas Unsicherheit: 41,30 %).

3 Datenschutz bei Daten aus dem Internet of Things

Bei der Betrachtung der betrieblichen IT-Sicherheit liegt der Fokus der Unternehmen häufig noch immer auf den Daten. Die dahinterliegende Grundannahme zur Ermittlung des Schutzbedarfes – der Angreifer will das, was uns am Wichtigsten ist – ist im Bereich des Internet of Things jedoch zu einseitig. Schutzwürdig ist im IoT nicht nur das „Was“, also die Daten (asset-driven), sondern ganz besonders auch das „Wie“, sprich der dahinterliegende Prozess (threat-driven).

Für ein konkretes Endergebnis einer Betrachtung der IT-Sicherheit in Form von konkreten Maßnahmen und Methoden ist ein datenzentrierter Ansatz jedoch deutlich einfacher. Auch die Abgrenzung gelingt akkurater, wobei sich im IoT-Umfeld häufig die Frage stellt, wo die Betrachtung endet, beispielsweise, ob Schnittstellen mitbetrachtet werden oder außen vor bleiben. Geht man von den IT-Schutzzielen Integrität, Verfügbarkeit und Vertraulichkeit aus, so kann lediglich eines dieser Ziele durch die alleinige Betrachtung der Daten verfolgt werden und zwar das der Verfügbarkeit. Für die weiteren Schutzziele der Integrität und Vertraulichkeit müssen zwingendermaßen die dahinterliegenden Prozesse mitbedacht werden. Somit kommt bei einem reinen Daten- bzw. Informationssystem ein datenzentrierter Ansatz in Frage. Bei einem Steuerungssystem hingegen stößt dieser Ansatz an seine Grenzen, während eine prozesszentrierte Herangehensweise funktioniert.

All diese Aspekte gilt es für das IoT zu berücksichtigen, weshalb die Thematik im Rahmen eines Workshops bearbeitet werden soll. Ein Vortrag zur Verinnerlichung dieser sowohl komplexen als auch spannenden Thematik wäre weniger effizient. Gleichzeitig sei jedoch angemerkt, dass die für das Themenfeld IoT ebenfalls zwingend zu betrachtende Safety (als Teil der IT-Sicherheit) im Rahmen des Workshops nicht behandelt wird.

4 Schwachstellenanalyse IoT

Neben der Behebung bekannter Ursachen für die Problemanfälligkeit des IoT – beispielsweise die Veröffentlichung von noch im Beta-Stadium befindlichen Produkten, mangelhaftes Qualitätsmanagement sowie fehlende kurz- und langfristige Verwaltung – können UUX-Professionals bereits bei der Entstehung solcher Produkte und Prozesse für Usable Security & Privacy sorgen, indem beispielsweise die Vergabe der Voreinstellungen optimiert wird.

Inwieweit Daten aus dem IoT frei zugänglich sind, verdeutlicht etwa die Suchmaschine Shodan, welche sich selbst als „die weltweit erste Suchmaschine für internetfähige Geräte“ bezeichnet [6]. Gefunden werden können alle Geräte wie Router, Server oder Webcams, welche mit dem Internet verbunden sind. Durch eine einfache Suche wird das Defizit im Umgang mit betrieblichen aber auch mit privaten Daten aus dem Smart-Home-Bereich deutlich.

So veröffentlichte Martin Hron im August 2018 einen Blogartikel, in welchem er die Schwächen von IoT-Geräten visualisierte, welche das Message Queuing Telemetry Transport Smart Device Communications Protocol (MQTT) nutzen. Dabei fand er mittels Shodan über 49.000 fehlerhaft konfigurierte MQTT-Server (siehe Abbildung 1). Darunter waren auch mehr als 32.000 über das Internet frei zugängliche Server ohne Passwortschutz, zu welchen sowohl betriebliche als auch private Smart-Home-Geräte zählten [7].

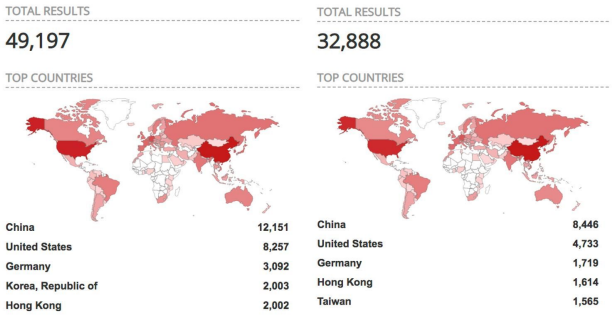

Abbildung 1: MQTT-Server, die auf Shodan gelistet sind [8]

Die Einführung intelligenter Messsysteme (Smart Grid) und die gegenläufigen Interessen der diversen Stakeholder – Netzbetreiber, Energieversorgungsunternehmen, Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie Endkunden – bieten zahlreiche Herausforderungen. Die Smart Grids bestehen aus digitalen Stromzählern (Smart Meter) und Smart Meter

Gateways, welche die sichere Kommunikation der Smart-Meter-Daten gewährleisten sollen. Durch die digitale Erfassung von Verbrauchswerten auf Abnehmerebene, die nahezu in Echtzeit stattfindet, verspricht sich der Netzbetreiber auf der einen Seite eine effizientere Lenkung des Stroms. Gleichzeitig wünscht der Energieversorger ein exaktes Lastenmanagement, so dass weniger überschüssige Energie vorgehalten werden muss. Auf der anderen Seite setzt das BSI enge technische Vorgaben, um die Sicherheit der Stromversorgung als kritische Infrastruktur zu gewährleisten. Der Verbraucher wiederum kann durch niedrigere Stromkosten, flexible Tarife und ansprechendes Energie-Feedback auf Basis von Webtechnologien profitieren. Aus Sicht des Verbraucher- bzw. Datenschutzes gilt es zu bedenken, dass die Übertragung von Stromverbrauchsdaten Rückschlüsse auf Verhaltensmuster sowie andere Informationen, beispielsweise die Personenanzahl im Haushalt, zulassen können. Für ein solches Szenario könnte ein UUX-Professional folgende Aufgabenstellung zu bewältigen haben: Wie können unterschiedliche und konkurrierende Anforderung der Stakeholder an ein digitales Produkt bzw. einen Service zusammengebracht werden und eine Lösung entwickelt werden, welche für alle Stakeholder möglichst gebrauchstauglich und zugleich aus datenschutzrechtlicher Sicht optimal ist?

Die Suchmaschine Shodan ermöglicht mittels eines Browsers nicht nur die Abfrage und Anzeige von Daten unzähliger Geräte und Systeme, die über das Internet vernetzt sind, sondern je nach Einhaltung von Sicherheitsstandards auch die Bedienung der gefundenen Server. Dazu zählen beispielsweise auch die oben dargestellten Smart Grits, Smart-Home-Geräte wie Heizungssysteme oder Überwachungskameras, kritische Infrastrukturen wie Strom- oder Wassernetze, aber auch Verkehrsinfrastrukturen wie Ampelsysteme [8]. Die Vernetzung endet jedoch nicht in der immobilen Welt.

Daten werden auch im mobilen Bereich ermittelt, verarbeitet und zur Verfügung gestellt. So wird bei Fahrzeugen – neben Kriterien wie Leistung, Nachhaltigkeit und Design – die Fahrerassistenz immer häufiger zu einem Verkaufsargument. Die dazu notwendigen Konnektivitätsfunktionen beruhen ebenfalls auf einem Austausch von Daten zahlreicher Sensoren, Steuerungselemente und angebundener Systeme. Genutzt werden können diese Daten sowohl von natürlichen Personen und Unternehmen als auch von Systemen innerhalb und außerhalb des Fahrzeugs. Zu den potentiellen Nutzern bzw. Nutznießern solcher Daten zählen elektronische Geräte, Verkehrsinfrastrukturen, Fahrzeugbesitzer und -eigentümer, Fahrer und Fahrgäste, andere Verkehrsteilnehmer, Behörden, Hersteller, Kfz-Versicherungsanbieter usw. Mit der steigenden Anzahl an Akteuren ist die Spannbreite an Bedürfnissen mit einer gleichzeitigen Verbindung der jeweils geltenden datenschutzrechtlichen Anforderung ebenfalls gewachsen.

Nach den Empfehlungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit [9] soll das Recht auf informationelle Selbstbestimmung auch für Fahrzeugnutzer gelten und datenschutzfreundliche Voreinstellungen üblich sein. Zudem soll transparent gemacht werden, welche Daten auch ohne Einwilligung des Fahrzeugnutzers aufgrund eines Gesetzes verarbeitet werden dürfen. Gleichzeitig soll bei der Verarbeitung von Fahrzeugdaten auch der Grundsatz der Datenvermeidung und Datensparsamkeit gelten. Hinzukommen technische Anforderungen wie eine wirksame Verschlüsselung und Anonymisierung der Daten [10]. Diese und ähnliche Anforderungen nutzerfreundlich zu realisieren, stellt einen UUX-Professional stets aufs Neue vor spannende Herausforderungen.

5 Datenschutz bei Daten auf Plattformen

Große internationale Plattform-Anbieter wie Google [11], Facebook [12] oder Microsoft [13] haben bereits vor dem Wirksamwerden der DSGVO-Regelungen damit begonnen, ihren Nutzern Möglichkeiten zur Verfügung zu stellen, mit welchen sie den Schutz ihrer Daten selbst verwalten können. Ausschlaggebend für die Entwicklung und Integration dieser Datenschutz-Dashboards war meist die anhaltende Kritik von Seiten der Nutzer, von Regierungsbehörden oder auch Medien [14]. Nutzern dieser Plattformen wird nun ermöglicht, mittels des Dashboards einzustellen, welche Daten die Plattformanbieter speichern beziehungsweise auswerten dürfen (z. B. Bewegungsprofile, Produktinteressen, Suchanfragen oder Kommunikationsdaten), aber auch welche Informationen für andere Nutzer sichtbar sind. Von verschiedenen Seiten wird jedoch kritisiert, dass die Voreinstellungen in diesen Dashboards zu intransparent und nicht datenschutzfreundlich genug seien [15].

Facebook hat nach einem massiven Datenskandal im März 2018 damit begonnen, die Verbesserung der Datensicherheit und Privatsphäre voranzutreiben [16]. Dabei wurden zunächst die Einstellungen zur Sicherheits- und Privatsphäre komplett überarbeitet, sodass die Nutzer nun umfassendere Informationen zur Konfiguration ihrer persönlichen Einstellungen, zur Account-Sicherheit und zur Nutzung ihrer personenbezogenen Daten erhalten.

Google bietet seinen Kunden eine Transparenzschnittstelle an, mit deren Hilfe diese in die Lage versetzt werden, getätigte Suchanfragen, Standortverläufe usw. einzusehen und zu löschen. Zusätzlich stellt Google einen Privatsphärecheck [17] zur Verfügung, einen Wizard, mit dem die eigenen Einstellungen zur Privatsphäre für den gesamten Google-Account verwaltet werden können.

Das Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO [18] erfüllt Google mit dem Onlinedienst Google Takeout [19]. Dieser Dienst ermöglicht es registrierten Google-Nutzern, eine Kopie ihrer personenbezogenen Daten aus den von ihnen verwendeten Google-Diensten, wie beispielsweise Gmail, Google Kalender oder Google Fotos, zu exportieren. Die gewünschten Daten können ausgewählt und in gängigen Archivformaten wie JSON, CSV, HTML oder mbox heruntergeladen werden. Dadurch bietet sich registrierten Nutzern die Möglichkeit, ihre Daten zu sichern oder für die Nutzung in einem anderen Dienst zu verwenden.

In einer aktuellen Studie [20] wurden knapp zehn bekannte Social-Media-Anbieter und vergleichbare Plattformen in Bezug auf ihre Stärken und Schwachpunkte hinsichtlich des Datenschutzes analysiert. Das Ergebnis: Die Einstellungsmöglichkeiten sind oft versteckt. Der Nutzer wird

häufig mit schwammigen Formulierungen und „Wohlfühltexten“, die Datenschutz suggerieren („Ihre persönlichen Daten sind bei uns sicher …“, „Wir verdienen uns Ihr Vertrauen Tag für Tag …“ [21]), in einer vermeintlichen Sicherheit gewogen. Die Voreinstellungen entsprechen oft nicht dem Privacy-by-Default-Prinzip, beispielsweise bei der Sichtbarkeit von Profilen oder Beiträgen. Auch erlauben die Voreinstellungen meist die Nutzung der Daten für personalisierte Werbung, Tracking oder Gesichtserkennung, aber auch für die Nutzung durch Drittanbieter, Einblendung des Profilbilds in Werbeanzeigen und Ähnliches. Ebenfalls als problematisch ist anzusehen, dass viele Plattform-Anbieter auch außerhalb ihres Netzwerks Daten erfassen. Zudem werden häufig Funktionen angeboten, durch die möglicherweise die Privatsphäre Dritter verletzt wird, beispielsweise die Möglichkeit eines Adressbuch- oder Kalenderabgleichs.

6 Workshop des Arbeitskreis Usable Security & Privacy der German UPA

Im Workshop wird aufgrund der oben aufgezeigten Herausforderungen ein Ansatz vorgestellt, mit welchem personenbezogene Daten – beispielweise IoT-Daten aus den Bereichen Smart Metering, Smart Home oder Smart Car bzw. Benutzerprofildaten wie aus Googles Takeout – in einem anbieterunabhängigen Dashboard aufbereitet, visualisiert und damit verständlicher und zugänglicher werden. Durch diesen Ansatz sollen Anwender sowie Unternehmen in die Lage versetzt werden, bewusste Entscheidungen auf einer soliden Datenbasis zu treffen und damit einhergehend auch souverän mit ihren (bzw. den ihnen anvertrauten) personenbezogenen Daten umgehen zu können.

Das Dashboard zur Analyse des Google Takeouts umfasst folgende Features:

Person: Übersicht über alle Identitäten, beispielsweise Adressinformationen aus Onlineshops; Google speichert diese Daten, um sie bei der Bestellung in einem anderen Shop im Browser vorschlagen zu können.

Historie: Kompletter Browserverlauf mit Seitenaufrufen (Titel, URL), Lesezeichen sowie Prozentauswertung der besuchten Webseiten mit bzw. ohne SSL-Verschlüsselung (siehe Abbildung 2).

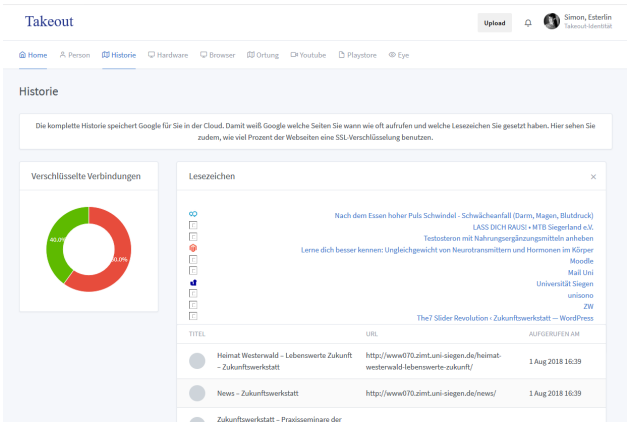

Abbildung 2: Google-Takeout-Analysedashboard: Historie

Hardware: Übersicht aller aktuell bzw. früher genutzten Android-Geräte, jeweils mit Geräte-IDs, IP-Adresse und Datum der Erstnutzung.

Browser: Übersicht aller installierten Browsererweiterungen, jeweils mit Name, Version, Update-URL und Status (aktiviert/deaktiviert, im normalen wie im Inkognitomodus).

Ortung: Karte sowie Liste (jeweils mit Name, GPS-Koordinaten und Speicherdatum) aller Lieblingsorte, welche auf den genutzten Android-Geräten gespeichert wurden.

You Tube: Übersicht der bei You Tube aufgerufenen Videos.

Play Store: Auflistung aller Apps und digitalen Inhalte, welche bei Google Play gekauft wurden. Die Einträge im Bestellverlauf umfassen jeweils Produktname, Typ (z. B. Abonnement, Apps, inApp-Käufe), Datum, Rechnungsempfänger und Preis (siehe Abbildung 3).

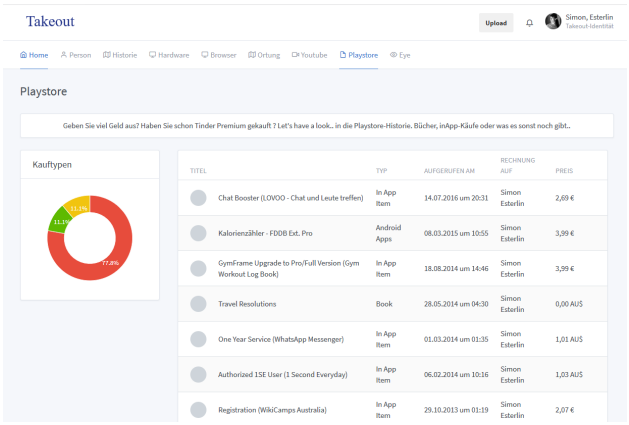

Abbildung 3: Google-Takeout-Analysedashboard: Play Store

Eye: Darstellung sämtlicher Standortdaten, die erhoben wurden, während der Standortverlauf aktiviert war; aufbereitet in Form

einer Karte und einer Liste, jeweils mit der Angabe von Datum, Uhrzeit und GPS-Koordinaten (siehe Abbildung 4).

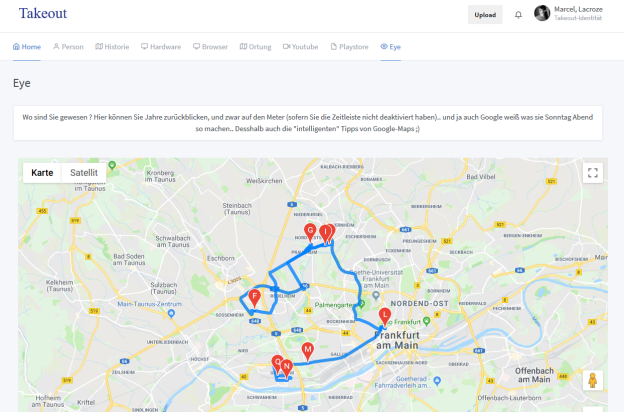

Abbildung 4: Google-Takeout-Analysedashboard: Eye

Im Workshop werden gemeinsam mit den Teilnehmern Beispieldaten in diesem Visualisierungstool exploriert. Anhand umfassender Beispiele werden Einblicke gegeben, wie die Daten korrekt interpretiert, aber auch hinterfragt und im jeweiligen Kontext zielbewusst eingesetzt werden können (Data Literacy). Des Weiteren wird mit den Teilnehmern diskutiert, welche konkreten Herausforderungen sich bei der Gestaltung von Lösungen für den benutzerfreundlichen Datenschutz für Unternehmen ergeben – Herausforderungen aus Sicht von Herstellern und Diensteanbietern, aber auch Anwenderunternehmen.

7 Agenda des Workshops

Im Rahmen des 90-minütigen Workshops wird ein Erfahrungsabgleich mit den Teilnehmenden zu folgenden Themen durchgeführt:

- Vorstellung des Visualisierungswerkzeugs/Dashboards, mögliche Einsatzbereiche und -szenarien;
- gemeinsame Nutzung des Visualisierungswerkzeugs mit den Teilnehmern, Datenanalyse und Interpretation;
- Diskussionen mit den Teilnehmern: Datenkompetenz, Umsetzung der DSGVO, Folgen für Unternehmen;
- Anwendbarkeit bekannter Usability-Methoden und -Werkzeuge auf den Bereich Usable Privacy; Future Work: Bedarf nach Anpassungen bzw. Erweiterungen von Methoden und Werkzeugen

Außerdem werden im Rahmen des Workshops der Arbeitskreis Usable Security & Privacy, seine Themen, Ziele und Akteure sowie deren Projekte kurz vorgestellt. Die Hauptzielgruppe des Workshops sind UUX-Professionals, welche selbst beruflich im Themenumfeld Usable Security & Privacy aktiv sind bzw. eventuell in Zukunft sein werden. Der Workshop ist aber auch geeignet für interessierte Einsteiger, die sich über die Themen Datenvisualisierung, Data Literacy, Usable Security & Privacy oder die Arbeit des Arbeitskreises informieren möchten. Die Ergebnisse des Workshops werden im Nachgang in einer geeigneten Form aufbereitet und den Teilnehmern zur Verfügung gestellt bzw. veröffentlicht.

8 Arbeitskreis Usable Security & Privacy der German UPA

Der Arbeitskreis Usable Security & Privacy beschäftigt sich seit 2015 mit Ansätzen und Konzepten, welche sicherheits- und/oder privatheitsfördernde Verfahren für Software und interaktive Produkte stärker an den Zielen und Aufgaben der Nutzer ausrichten und welche dafür sorgen, dass Funktionsweisen von Sicherheitselementen auch für Nichtexperten verständlich gemacht werden. Ziel des Arbeitskreises ist es dabei, sowohl bei UUX-Professionals als auch bei Nutzern im privaten und beruflichen Umfeld ein verstärktes Bewusstsein für das Themengebiet Usable Security & Privacy zu schaffen.

Um die Arbeit der UUX-Professionals zu unterstützen, wird das vorhandene Fachwissen aus wissenschaftlicher Forschung und beruflicher Praxis zusammengeführt und damit eine Brücke zwischen der Arbeit der UUX-Professionals und anderen Disziplinen, wie dem Security Engineering, geschlagen.

DANKSAGUNG

Die Autoren dieses Textes danken den übrigen Mitgliedern des Arbeitskreises Usable Security & Privacy. Teile dieser Arbeit sind im Rahmen des Forschungsprojektes „TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen“ [22] entstanden.

REFERENZEN

[1] https://eur-lex.europa.eu/eli/dir/2016/680/oj
[2] https://dejure.org/gesetze/DSGVO/1.html
[3] https://dejure.org/gesetze/DSGVO/25.html
[4] https://blog.f-secure.com/podcast-gdpr-one-year-later
[5] https://germanupa.de/berufsverband-german-upa/aktuelles/usable-security-privacy-ergebnisse-upa-mitgliederbefragung
[6] https://www.shodan.io/
[7] https://blog.avast.com/mqtt-vulnerabilities-hacking-smart-homes
[8] https://help.shodan.io/
[9] https://www.bfdi.bund.de/
[10] https://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/DatenschutzrechtlicheEmpfehlungenVernetztesAuto.pdf?__blob=publicationFile&v=1
[11] https://www.google.com/
[12] https://www.facebook.com/
[13] https://www.microsoft.com/
[14] https://www.theguardian.com/techno-logy/2014/may/22/facebook-privacy-settings-changes-users
[15] https://www.e-recht24.de/artikel/datenschutz/6449-facebook-datenschutz-so -sichern-sie-ihre-daten.html
[16] https://me-meburn.com/2018/03/facebook-new-privacy-settings/
[17] https://myaccount.google.com/intro/privacycheckup?hl=de
[18] https://dejure.org/gesetze/DSGVO/20.html
[19] https://takeout.google.com/
[20] Polst, S. et al. (in print), Company Privacy Dashboards: Employee Needs and Requirements. Proceedings of the HCI International 2019.
[21] https://account.microsoft.com
[22] https://www.trusd-projekt.de/

DIE AUTOREN

Hartmut Schmitt ist Koordinator für Forschungsprojekte beim saarländischen IT-Lieferanten HK Business Solution GmbH. Er ist seit 2006 in Verbundvorhaben auf den Gebieten Mensch-Computer-Interaktion, Usability/User Experience und Software-Engineering tätig, u. a. als Projektkoordinator in mehreren BMBF- und BMWi-geförderten Verbundvorhaben.

Mandy Balthasar ist wissenschaftliche Mitarbeiterin an der Universität der Bundeswehr München am Institut für Softwaretechnologie. Als IT-Consultant und zertifizierte Datenschutzbeauftragte wirkte sie in den Centern of Competence Web Technologies und User Experience mit und legt dabei ihren Themenfokus auf Datenschutz, Mensch-Computer-Interaktion, Usability und User Experience sowie Software-Engineering und Kryptographie. Dabei hat sie in unterschiedlichen Rollen, als Entwicklerin, IT-Security-Consultant und Security Managerin mitgewirkt. Außerdem ist sie als Lehrende an verschiedenen Hochschulen und Fachhochschulen sowie für die Springer Nature Campus GmbH im Einsatz.

Timo Jakobi ist wissenschaftlicher Mitarbeiter an der Universität Siegen und der Hochschule Bonn-Rhein-Sieg. Sein Forschungsschwerpunkt liegt auf der Entwicklung gebrauchstauglicher Unterstützungsmechanismen für das Management von Privatsphäre in IKT-Anwendungen. Hier stellt insbesondere der Trend zum Internet of Things mit der Anbindung und Analyse unterschiedlichster und abstrakter Daten(-quellen) eine neue Herausforderung dar, um Anwendern Transparenz und Kontrolle über die eigenen Daten zu verleihen.