Eberhard Zehendner

Workshop „Handys – aber sicher!“

Der Workshop fand am Sonntag, den 22. Oktober 2017 von 8:00 bis 11:30 Uhr in einem Seminarraum der Friedrich-Schiller-Universität Jena statt. Es hatte im Vorfeld aus dem FIfF-Vorstand Bedenken gegeben, ob den Besucherinnen und Besuchern der FIfFKon eine derart frühe Anfangszeit zugemutet werden könne. Nachträglich kann ich nun ja zugeben, dass der an mich herangetragene Pessimismus dann auch mich etwas verunsicherte. Und so sah ich denn mit einer gewissen Nervosität der Eröffnung des Workshops entgegen, zumal wir am Abend zuvor noch bis 23 Uhr den Film „Zero Days“ gezeigt hatten. Doch der Seminarraum füllte sich zunehmend, und mit etwa 25 Anwesenden konnte es nun losgehen.

Die Teilnehmenden konnten über die Inhalte des Workshops höchstens spekuliert haben, da ich zwar den Workshop-Titel verbreitet, aber keine näheren Ausführungen zur Ausgestaltung hatte verlauten lassen. Nun gut, auf den beiden vorangehenden Konferenztagen hatte ich, im persönlichen Gespräch, die eine oder andere Konkretisierung erkennen lassen. Mit Gates'scher Chuzpe hätte ich ja nun behaupten können, der Informationsmangel sollte als Feature des Veranstaltungskonzepts verstanden werden. Das war er natürlich nicht. Aber ich hatte Glück im Unglück: Denn das Konzept, das ich ursprünglich verbreiten wollte, sah ganz anders aus als der tatsächliche Ablauf des Workshops. Ich hatte nämlich mit folgender Formulierung (die auch für eine breite Ankündigung gedacht war) bei etlichen Kandidatinnen und Kandidaten einige Wochen vor Beginn der Konferenz um Mithilfe im Workshop geworben:

> *„Der Workshop richtet sich vorwiegend an Jugendliche mit eigenem Handy. Es sollten dort praktische Elemente der IT-Sicherheit demonstriert und auf den individuellen Geräten eingerichtet werden, vor allem E-Mail-Verschlüsselung, sichere Messenger, Sicherheitseinstellungen und das Unterbinden von Datenabfluss. Lässt sich sicher auch in Teilen als eine Keysigning-Party gestalten. Wichtig wäre mir, dass auch das Zusammenspiel unterschiedlicher Plattformen klappt.“*

Der Rücklauf war dann doch ziemlich verhalten. Insbesondere schienen die meisten der Angesprochenen ihr Gerät unter Android zu betreiben, die nötige Breite für eine derart vollmundige Ankündigung wollte sich also nicht einstellen. Und so gab es denn auch keine detaillierten Werbemaßnahmen. Aus der ursprünglich eher wie ein Tutorium konzipierten Veranstaltung wurde eine lockere Gesprächsrunde, die dennoch das wichtigste Kriterium eines *Workshops* unzweifelhaft aufwies – es wurde heftig gearbeitet.

Themenfindung

Zunächst hatten alle Anwesenden die Möglichkeit, ihre Sichtweise auf den Problemkreis „Handy-Sicherheit“ darzustellen und bestimmte, sie vorwiegend interessierende Fragestellungen einzubringen. Dies führte schließlich auf eine ebenso umfangreiche wie bunte Themensammlung (Abbildung 1). Es wurde aus dem Kreis der Anwesenden darauf hingewiesen, dass zunächst *Ziele* formuliert werden müssten, an denen sich Beurteilungen ausrichten können.

Aus der Fülle der Themen schälten sich gewisse Bereiche als besonders interessant heraus, diese wurden dann vertieft diskutiert. Dies war zunächst der Komplex „Google“ mit folgenden Einzelfragestellungen:

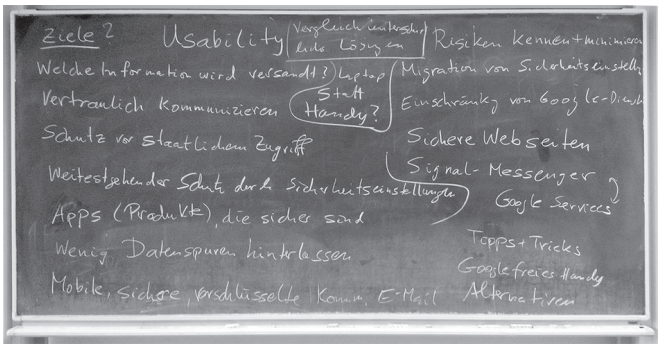

Abbildung 1: Themensammlung

- Inwieweit (und wie) können Google-Dienste eingeschränkt werden?
- (Wie) hängt der Signal-Messenger mit den Google Services zusammen?
- Wie kommen wir zu einem Google-freien Handy?
- Welche Alternativen zu Google auf dem Handy gibt es?

Ein weiterer Komplex betraf die *Vertraulichkeit der Kommunikation per Handy,* mit den Unterpunkten

- Verschlüsselung
- Sicherheit der Maßnahmen

sowie (auch andere Bereiche betreffend)

- Welche Information wird versandt?
- Wenig Datenspuren hinterlassen
- Schutz vor staatlichem Zugriff
- Apps (Produkte), die sicher sind

Dabei bestehen relevante Unterschiede zwischen der Kommunikation per E-Mail bzw. über einen Instant-Messenger.

Der Komplex *Geräteschutz* mit den Punkten

- Zugriffsschutz
- Produkte
- weitestgehender Schutz durch Sicherheitseinstellungen
- Migration von Sicherheitseinstellungen

konnte aus zeitlichen Gründen nur angerissen, aber nicht vertieft werden, desgleichen die übergreifenden Themen

- Vergleich unterschiedlicher Lösungen
- Risiken kennen und minimieren
- Tipps und Tricks
- Wie stark schränken Sicherheitsmechanismen die Usability ein?
- Sichere Webseiten
- Sind Handys sicherheitstechnisch so bedenklich, dass die Verwendung eines Laptops die angemessene Konsequenz ist?

Bedingt durch den Beginn parallel zum Workshop abgehaltener Vorträge wechselten nun einige der Anwesenden dorthin. Nach einer angemessenen Pause wurde der Workshop in kleinerer Runde fortgesetzt. Es dominierten nun speziellere Fragen das Gespräch, der Informationsstand erschien mir bereits sehr hoch. Der Begriff „Expertenrunde" wäre dafür vielleicht angemessen.

Handy ohne Google

Die Diskussion konzentrierte sich nun zunächst auf das Thema „Handy ohne Google" und kreiste dabei um folgende Fragestellungen (siehe Abbildung 2):

- Welche Betriebssysteme kommen als Google-freie Alternativen in Frage?
- Wie ist der Wechsel des Betriebssystems technisch zu vollziehen?
- Welche Recovery-Systeme kommen in Frage?
- Bestehen derartige Möglichkeiten auch für ältere Smartphones?
- Wird durch einen Wechsel die Herstellergarantie für das Gerät beeinträchtigt?
- Sind nach einem Wechsel weiterhin Updates möglich?
- Woher bekomme ich ohne Google meine Apps?
- Wo liegen meine bisherigen Daten?

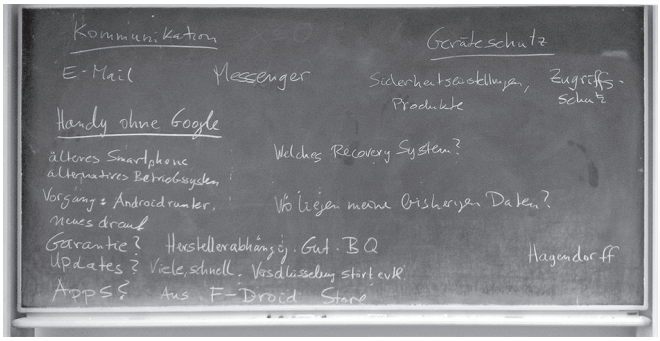

Abbildung 2: Vertiefung von Themen

Mobile Instant-Messenger

Nun wandte sich die Diskussion der Frage zu, welche Anforderungen an einen *mobilen Instant-Messenger* zu stellen seien und welche Anwendungen diese erfüllen könnten. Zunächst wurden die Anwesenden gebeten, an der Tafel (Abbildung 3) ihre persönliche Situation im Schema „Ich verwende … weil …" einzutragen. Dies ergab dann eine Zusammenstellung wie in Tabelle 1 (die Schreibweise dort sowie in den nachfolgenden Ausführungen orientiert sich an offiziellen Quellen und weicht dadurch teilweise vom Tafelbild ab).

Ich verwende …	weil …
Line	ich mit Asien schreibe
Signal	Open Source, verschlüsselt
Telegram	alle Freunde diesen verwenden
iMessage	
Conversations	besserer Metadatenschutz
Gajim	besserer Metadatenschutz
ChatSecure	
keinen	**keiner mich überzeugt**
WhatsApp	Gruppenzwang
Threema	verschlüsselt, simple, Schweiz, keine Telefonnummern
Facebook	Gruppe

Tabelle 1: Nutzung von mobilen Instant-Messengern durch Workshop-Teilnehmende und ihre Begründung

Die vorangestellten Striche im Tafelbild lassen erkennen, dass es eine Präferenz für *Threema* gab, gefolgt von *WhatsApp*. Ansonsten schienen die Anwesenden dann jeweils „ihren" persönlichen Messenger (manchmal auch mehrere) zu benutzen. Sicherheitsaspekte spielen anscheinend nur teilweise eine Rolle bei der Auswahl; ebenso entscheidend ist die „Community", mit der kommuniziert werden soll. Es könnte sogar sein, dass letzteres auch für die Wahl eines Messengers höherer Sicherheit (mit-)verantwortlich ist, falls „meine Community" dies von mir erwartet.

Besonders interessant fand ich die Antwort „Ich verwende keinen (Messenger), weil keiner mich überzeugt". Diese kam von einem Teilnehmer, der sich beruflich mit der Nutzung von Smartphones im gewerblichen Bereich beschäftigt. Dort wurden zu einem sehr frühen Zeitpunkt die Maßstäbe durch das *BlackBerry* geprägt, und generell liegen die Anforderungen an Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit im gewerblichen Bereich höher als im privaten.

Die Aufzählung wurde dann noch erweitert um lediglich gelegentlich genutzte Messenger sowie solche, die evtl. auch noch von Interesse sein könnten. Dies ergab dann folgende Zusatzliste:

- SIMSme
- ICQ
- Riot
- Skype
- Hangouts
- qTox
- Briar
- Ring

Von einigen dieser Messenger hatte ich noch nie gehört. Daher habe ich im Nachgang ein wenig recherchiert und zunächst eine umfangreiche „Liste von mobilen Instant-Messengern" (*https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Mes-*

sengern) mit Übersicht vieler Eigenschaften im Netz gefunden, die anscheinend noch laufend gepflegt wird. Doch selbst diese Übersicht führt nicht alle genannten Messenger auf. Es lohnt sich, dazu weiter im Netz zu stöbern und sich die tatsächlich interessanten Ansätze genauer anzusehen, zum Beispiel für *Briar* (*https://motherboard.vice.com/de/article/7xenwb/diese-app-will-den-messenger-markt-revolutionieren*) oder *Riot* (*https://www.deathmetalmods.de/messaging-und-open-source-ein-kurzer-blick-auf-riot-im-gastbeitrag/*).

Als Alternativen zur Verwendung eines mobilen Instant-Messengers wurde im Workshop auch die Kommunikation über *SMS* oder *E-Mail* genannt. Bemerkenswerterweise wurden bekannte Messenger wie *Signal* oder der von *Facebook* bereits um die Möglichkeit erweitert, dort direkt SMS verarbeiten zu können. Zum Abschluss sei daher noch auf eine (allerdings nicht ganz aktuelle) Übersicht zu „Sicherheit und Nachhaltigkeit von WhatsApp, E-Mail, SMS & Co." hingewiesen, zusammengestellt von der „Digitalen Gesellschaft" der Schweiz: *https://www.digitale-gesellschaft.ch/messenger/bewertung.html*.

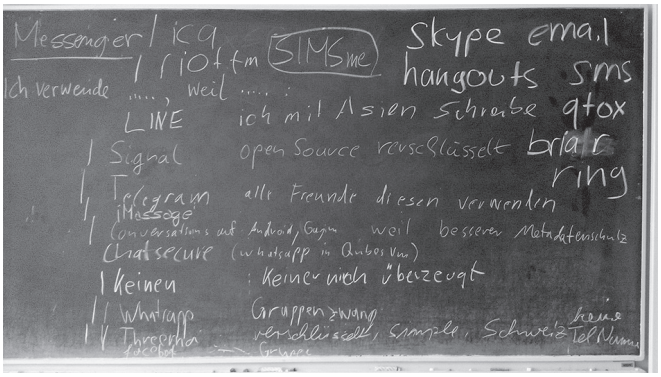

Abbildung 3: Tafelanschrift zur Nutzung von mobilen Instant-Messengern

Eberhard Zehendner

Workshop „IT-Sicherheit barrierefrei"

Der kleine, aber feine Workshop wurde mitveranstaltet von Henning Lübbecke, Sprecher der Fachgruppe „Informatik und Inklusion" im Fachbereich Informatik und Gesellschaft der Gesellschaft für Informatik (GI) und im FIfF schon bestens ausgewiesen durch seinen Workshop „Teilhabe an der allgegenwärtigen Kommunikation" auf der FIfFKon 2015 in Erlangen. Es war uns eine besondere Freude, den Beauftragten der Thüringer Landesregierung für Menschen mit Behinderungen, Joachim Leibiger, im Workshop begrüßen zu dürfen. Insofern hatte der Workshop eindeutig einen Vernetzungscharakter. Er war auch so konzipiert, die Zusammenarbeit zwischen der Fachgruppe „Informatik und Inklusion", dem FIfF, verschiedenen Landesverbänden und öffentlichen Beauftragten für die Belange von Menschen mit Behinderungen sowie interessierten Hochschulen mit einschlägigen Forschungsansätzen zu stärken.

IT-Sicherheit ist ein sehr sensibler Bereich, denn es geht unter anderem um persönliche Daten, den Schutz der eigenen digitalen Identität, Abwehr von betrügerischen Manipulationen, Zugang zu vertraulichen Unterlagen und nicht zuletzt den Zugriff auf das eigene Konto. Anders als Herr und Frau Mustermann, auf die gängige Hard- und Software für IT-Sicherheitszwecke typischerweise zugeschnitten sind, treffen Menschen mit Behinderung oft auf „Barrieren", die üblichen Mechanismen der IT-Sicher unmöglich machen. Das Problem t gerem Maße) auch Menschen mit der Schwelle einer amtlichen Behinderung, dazu zählen insbesondere viele ältere Menschen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Spannende Fragen in diesem Umfeld sind zum Beispiel:

- Wie lässt sich Barrierefreiheit „by design" erreichen? Also Systeme von Anfang an so zu planen und zu gestalten, dass Barrierefreiheit gegeben ist, nicht eingeschränkte Personen aber Einstellungen zur Steigerung der Arbeitsleistung und des persönlichen Wohlgefühls verändern können. Bisher ist es meist genau anders herum: Systeme werden für eine Hauptbenutzergruppe optimiert, für alle anderen werden (im besten Fall) nachträglich Hilfen zur Verfügung gestellt.

- Welche „Mitspieler" müssen angesprochen und überzeugt werden, um Fortschritte in der Barrierefreiheit zu machen? Wo geht das eher über die politische Schiene (Vorschriften), wo besser über freiwillige Aktivitäten (z. B. zwecks Profitmaximierung durch Ausweitung des Nutzerkreises eines Systems)?

- Welche erprobten (oder vielleicht auch noch unerprobten) Methoden, Mittel und Systeme stehen bereits zur Verfügung, um konkrete Schritte in Richtung Barrierefreiheit zu

2017 wurden konkrete Pläne ändergrenzen hinweg gefasst. Thematisch soll es dabei um sogenannte *Tastbare Displays* gehen, vgl. z. B.

- *https://www.elektronikpraxis.vogel.de/hmi/articles/543342/*,
- *https://d-nb.info/1076314538/34*,
- *https://tu-dresden.de/ing/informatik/institut-fuer-angewandte-informatik/mci/ressourcen/dateien/Dissertation_DenisePrescher.pdf*

Die neue Technologie ist den Betroffenen noch weitgehend unbekannt, hier ist über die Blinden- und Sehbehindertenverbände Aufklärungsarbeit zu leisten. Außerdem sind administrative Regelungen zur Versorgung zu treffen, die Technik muss weiterentwickelt und tauglich für die Massenfabrikation gemacht werden.