Dr. Markus Knasmüller
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informations- und Kommunikationstechnologie; Abteilungsleiter Entwicklung, BMD Systemhaus GmbH, Steyr

Zur Beweiskraft von elektronischen Nachrichten (SMS, E-Mail, Facebook und WhatsApp)

1. Einleitung

Elektronische Nachrichten, egal ob via SMS, Facebook, WhatsApp oder E-Mail, sind häufig Beweismittel vor Gericht. Vielfach stellt sich dabei die Frage, ob diese echt oder eventuell manipuliert sind. Der Autor hat bereits in der Ausgabe 4/2013 dieser Zeitschrift einen Artikel „Zur Echtheit und Manipulation von SMS“ geschrieben und dabei gezeigt, wie einfach es ist SMS zu manipulieren.[1]

SMS wird aber immer mehr durch andere Medien zurückgedrängt. Etwa führte die verstärkte Nutzung von Messaging-Diensten wie WhatsApp dazu, dass im 3. Quartal 2014 in Österreich nur mehr 1,078 Milliarden SMS verschickt wurden, während es im Vergleichszeitraum 2012 noch 1,835 Milliarden gewesen sind.[2] Daher setzt sich dieser Artikel verstärkt mit anderen, teilweise neueren Techniken auseinander und zeigt auf, ob und – falls ja – welche Manipulationen dabei denkbar sind.

Dementsprechend ist im Folgenden neben SMS auch E-Mail, Facebook und WhatsApp jeweils ein Abschnitt gewidmet. Der Autor baut dabei auf seine Erfahrung als Sachverständiger in verschiedenen Fällen auf, wo er die Echtheit derartigen Nachrichten prüfen musste. Auch wurde ihm dabei die Frage gestellt, ob es überhaupt grundsätzlich möglich wäre, diese zu fälschen, und – falls ja – ob dies nur Experten möglich wäre oder auch ein durchschnittlicher EDV-Anwender dies durchführen könnte.

2. SMS

SMS sind Kurznachrichten mit maximal 160 Zeichen, die (im Regelfall) per Mobiltelefon jederzeit einfach an einen Empfänger (im Regelfall ein anderes Mobiltelefon) versendet werden können. Aufgrund der Einfachheit und der hohen Akzeptanz haben sie eine große Verbreitung, wodurch es nicht verwunderlich ist, dass SMS auch in Gerichtsverfahren immer wieder eine bedeutende Rolle zukommt.

Vielfach stellt sich dann im Verfahren die Frage, ob eine SMS echt ist. Wenn bei Verhandlungen ein Handy mit einer SMS, die die Telefonnummer des Senders, die Sendezeit und den Text anzeigt, vorgezeigt wird, so sieht dies für einen technischen Laien nachvollziehbar aus. Dies umso mehr, da auch durch erste einfache Änderungsversuche (etwa mit Bearbeiten, Weitersenden etc die SMS ganz offensichtlich nicht manipuliert werden kann.

Ganz anders sehen aber die technischen Fakten aus. Eine Manipulation ist durchaus einfach möglich, wobei die einfachste Variante darin besteht, einfach vorzutäuschen, dass ein bestimmter Absender eine Nachricht übermittelt hat. Ist die Sendezeit egal, dann ermöglichen einschlägige Internetplattformen, wie etwas http://www.fakemysms.com, das Versenden, wobei die Absendernummer erfasst werden kann. Am Handydisplay sieht es dann so aus, als wäre tatsächlich die SMS von dieser Nummer versendet worden. Mit dieser Methode kann auch die Manipulation von einem Dritten, der gar keinen Zugang zu beiden Mobiltelefonen (Absender und Empfänger) hat, vorgenommen werden.

Aber auch ein nachträgliches Manipulieren einer empfangenen SMS ist möglich, indem die SIM-Karte manipuliert wird. Die SIM-Karte ist jene kleine Chipkarte, die sich in einem Mobiltelefon befindet und einerseits für die Identifizierung gegenüber der Mobiltelefongesellschaft verantwortlich ist (also angibt, mit welcher Telefonnummer jemand erreichbar ist), andererseits aber auch als (zumindest kleiner) Speicher dient. Auf einer SIM-Karte können bis zu 20 SMS gespeichert werden. Mittels eines einfachen Kartenlese- und -schreibgeräts, das im Internet um weniger als € 20,– erhältlich ist, kann der Inhalt der SIM-Karte ausgelesen werden. Unter Kenntnis des Formats einer SMS, also wie die einzelnen Hexadezimalzahlen angereiht werden, ist es dann (mehr oder weniger einfach) möglich, sowohl den Text als auch Datum und Uhrzeit einer SMS zu manipulieren.

So beginnt beispielsweise eine SMS, die von der Nummer +43 664 2127574 am 16. 6. 2012 um 19:59:48 Uhr versendet wurde, mit folgender Bytefolge:

01 06 91 34 66 04 05 F1 04 0C 91 **34 66 24 21 57 47** 00 00 **21 60 61 91 95 84** 80

Die relevanten Bytes sind dabei fett markiert, wobei die Informationen BCD-kodiert sind, also je 4 Bit ergeben eine Ziffer der Nummer und die Nummer beginnt jeweils im zweiten Halbbyte, das heißt, „34“ ist also als „43“ zu lesen, „57“ als „75“ etc.

Damit ist „34 66 24 21 57 47“ also als „43 66 42 12 75 74“ zu lesen, womit die Sendenummer sehr gut aus der Bytefolge erkennbar ist. Sollte nun eine andere Absendernummer vorgetäuscht werden, etwa die Nummer +43 676

4458367, so muss die Zeichenfolge „34 66 24 21 57 47“ einfach durch „34 76 46 54 38 76“ ausgetauscht werden.

So wie hiermit die Absendertelefonnummer geändert wurde, können auch Datum, Uhrzeit und in weiterer Folge auch der Inhalt der SMS manipuliert werden.

Abbildung 1 zeigt im Vergleich die beiden oben erwähnten SMS im Byteformat. Zuerst die SMS 0A von der Nummer +43 664 2127574 vom 16. 6. 2012 um 19:59:48 Uhr mit dem Text „Das“. Danach die SMS 0B von der Nummer +43 676 4458367 vom 10. 3. 2011 um 19:59:48 Uhr mit dem Text „Richtig gemein“.

```
0A: 01 06 91 34 66 04 05 F1 04 0C 91 34 66 24 21 57
    47 00 00 21 60 61 91 95 84 80 03 C4 F0 1C FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0A: 01 06 91 34 66 04 05 F1 04 0C 91 34 66 24 21 57
    47 00 00 21 60 61 91 95 84 80 03 C4 F0 1C FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
    FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Abbildung 1: Zwei verschiedene SMS im Byteformat im Vergleich

Auf einem handelsüblichen Handy würden die SMS am Display so dargestellt werden, dass hier die jeweils gewünschte Nachricht angezeigt wird. Dies zeigt Abbildung 2.

Je nachdem, welche Teile manipuliert worden sind, ist eine derartige Manipulation erkennbar, wobei wenn mit einem Dateneditor alle Bestandteile der SMS verändert werden, so ist die Manipulation nicht nachweisbar. Eine Garantie, dass eine bei Gericht vorgezeigte SMS also echt ist, ist daher auf keinen Fall gegeben, auch wenn eine derartige (nicht nachweisbare) Manipulation sicherlich einem durchschnittlichen EDV-Anwender nicht möglich wäre.

3. E-Mail

E-Mails in allen möglichen Variationen sind wahrscheinlich mittlerweile das häufigste Kommunikationsmedium überhaupt, gelten im Regelfall auch als schriftliche Vereinbarung und haben den gewöhnlichen Brief oder gar das Fax zu einem großen Teil bereits ersetzt.

Dabei ist der E-Mail-Begriff weit gefasst. Zwar gibt es für die E-Mail-Übertragung selbst ein definiertes Format, jedoch eine Vielzahl von verschiedenen Mailservern (zB Microsoft Exchange, Lotus Notes, GroupWise) und ebenso eine Vielzahl verschiedener Mailclients (zB Microsoft Outlook, Windows Live Mail, Mozilla Thunderbird). Die Speicherung der Nachrichten ist unterschiedlich, aber meist – zumindest im Hintergrund – in einfachem Textformat. Auch die Vorlage einer E-Mail passiert im Regelfall nicht durch Vorlage des Endgeräts (wie etwa bei einer SMS durch Hinterlegung des Mobiltelefons oder SIM-Karte), sondern durch Vorlage eines Ausdrucks. Es muss nicht weiter ausgeführt werden, dass diese dadurch nahezu beliebig manipuliert werden können. Um hier etwaige Veränderungen überprüfen zu können, müsste gegebenenfalls zumindest ein Zu-

Abbildung 2: Visualisierung der beiden SMS mit einem handelsüblichen Handy

griff auf den Mailserver vorhanden sein (was wohl nur im Strafrecht im Falle einer Hausdurchsuchung der Fall sein wird). Wobei auch hier nicht sichergestellt werden kann, ob die Nachrichten nicht geändert worden sind; in diesem Falle wäre eine Manipulation aber wohl nur durch einen Experten durchführbar und der E-Mail-Empfänger selbst hat – mangels Zugriffsrechten – oft wahrscheinlich gar nicht die Möglichkeit dazu.

Aber selbst wenn der Empfänger die E-Mail nicht verändert hat, könnte sie gefälscht sein, weil die Adresse des E-Mail-Absenders einfach vorgegeben werden kann. Auch hierfür gibt es Dienste, wie etwa http://www.fakemyemail.com, der analog zum bereits erwähnten http://www.fakemysms.com angewendet werden kann.

Abbildung 3 zeigt dabei die Erfassungsmaske. Es muss dabei also nur im Feld „Fake EMail“ die gewünschte Absender-E-Mail-Adresse eingegeben werden. Für den Empfänger sieht es dann so aus, als wäre tatsächlich die E-Mail von dieser Absenderadresse versendet worden. Die Kosten dafür sind minimal; für wenige Cent können Frei-

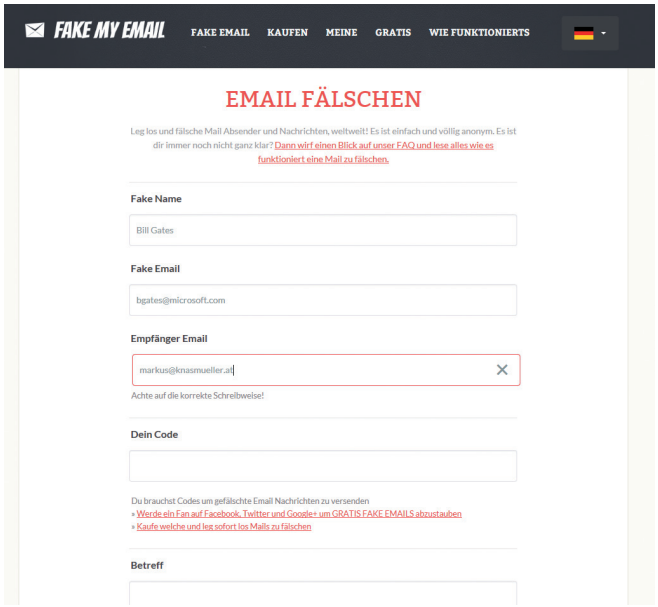

Abbildung 3: Absenden einer gefälschten E-Mail über die Internetplattform fakemyemail.com

schaltcodes gekauft werden, die für das Versenden der E-Mail notwendig sind.

Mit dieser Methode kann natürlich auch die Manipulation von einem Dritten, der gar keinen Zugang zu beiden Mailboxen (Absender und Empfänger) hat, vorgenommen werden.

Angemerkt sei aber, dass diese Art der Manipulation für den Empfänger kontrollierbar ist, weil der E-Mail-Header hier nicht korrekt wäre. Diese Information ist aber bei den Standardansichten der Mailclients, wie auch am Ausdruck, nicht enthalten und muss extra angesehen werden (in Outlook 2013 ist dies etwa über Datei/Informationen/Eigenschaften möglich). Sie sieht auszugsweise wie in Abbildung 4 dargestellt aus.

....
2015 19:19:35 +0200 (CEST)
Received: from pro-www12-v (pro-www12-v.intern.sms.at [192.168.20.195]) by mail.sms.at (Postfix) with ESMTP id 07C17A1BFC for <knasmueller@bmd.at>; Sat, 9 May 2015 19:19:35 +0200 (CEST)
To: <knasmueller@bmd.at>
From: mhk001 <mhk001@sms.at>
Subject: Testmail
Date: Sat, 9 May 2015 19:19:34 +0200
....

Abbildung 4: E-Mail-Header einer manipulierten E-Mail

Relevant sind dabei die mit „Received: from" bezeichneten Zeilen, mit denen der Weg der E-Mail verfolgt werden kann. Der Versender findet sich in der letzten „Received: from"-Zeile und es kann überprüft werden, ob diese mit dem tatsächlichen Mailserver des Absenders übereinstimmt.

Der Vollständigkeit halber sei noch angemerkt, dass es mittels digitaler Signaturen auch die Möglichkeit gibt, *de facto* manipulationssichere E-Mails zu versenden; jedoch wird dies noch sehr selten genutzt.

4. Facebook

Facebook ist wahrscheinlich das derzeit größte soziale Netzwerk. Jeder kann sich kostenfrei einen Account anlegen und online sogenannte „Freundschaften" schließen. Dabei ist es möglich, Statements („Postings"), Bilder oder auch Videos online zu stellen, die dann entweder alle Facebook-User oder aber auch nur ausgewählte Freunde sehen können. Auch können Nachrichten mit anderen Facebook-Usern ausgetauscht werden.

Diese Nachrichten enthalten leider auch immer wieder Beleidigungen, Drohungen oder aber auch Aussagen, die den Tatbestand der nationalsozialistischen Wiederbetätigung erfüllen, und sind somit Beweismittel in Gerichtsverfahren.[3]

Wesentlich ist, dass bei Facebook die Daten servergespeichert sind, also auf den Servern von Facebook liegen; somit können diese nicht lokal manipuliert werden, eine Veränderung durch einen anderen ist ausgeschlossen. Einzig der Urheber der Nachricht kann diese noch verändern oder löschen. Aber all das sind Ereignisse, die seitens Facebook verwaltet werden. Das heißt: Sofern eine Auskunft von Facebook gegeben wird (2014 war dies bei 109 Anfragen von österreichischen Behörden nur 16 Mal der Fall),[4] ist der Nachrichtenverlauf eindeutig nachvollziehbar. Ist eine derartige Auskunft nicht vorhanden, wovon also insbesondere vor einer Gerichtsverhandlung ausgegangen werden kann, ist es allerdings etwas problematischer.

In diesem Fall muss eine Beweissicherung einerseits einmal rasch erfolgen, da eben die Gefahr besteht, dass der Urheber die Nachrichten ändert oder löscht, und diese Informationen wären dann nicht mehr sichtbar. Andererseits kann eine Sicherung wohl nur durch Dateien, etwa mit der Funktionalität „Lade eine Kopie deiner Facebook-Daten herunter" oder Screenshots, erfolgen. Beides ist aber *de facto* beliebig manipulierbar. Es ist daher gegebenenfalls sicherlich sinnvoll, eine derartige Beweissicherung möglichst von einem unabhängigen Dritten durchführen zu lassen.

Zu beachten ist auch noch, dass eben jeder einen Account anlegen kann und der verwendete Name von Facebook nicht überprüft wird. Aus diesem Grund existieren unzählige sogenannte Fake-Profile, wodurch es oft nicht so einfach zu klären ist, welche Person tatsächlich dahinter steht (etwa könnte sich ein Dritter einfach einen Account unter dem Namen *Markus Knasmüller* anlegen und somit vom Autor versendete Nachrichten vortäuschen). Ein Beispiel dafür ist etwa die Facebook-Seite eines der wohl anerkanntesten Kriminalpsychologen Österreichs: Sachverständigenkollege Dr. *Thomas Müller* erzählt in Vortragen vielfach und hat dies auch dem Autor schriftlich bestätigt, dass es zwar eine Facebook-Seite unter seinem Namen gibt, mit der auch immer wieder Nachrichten versendet werden, er selbst habe aber keine angelegt und wisse gar nicht, wer wirklich dahintersteckt.

Aber auch wenn die Eigentümerfrage des Facebook-Accounts eindeutig geklärt werden kann, gibt es noch die Möglichkeit, dass ein Dritter sich die Zugangsdaten beschafft hat – oftmals einfach durch Erraten, bekanntlich ist ja das häufigste Passwort „123456"[5] –, und dann etwaige Facebook-Postings mit diesem Account im Namen des tatsächlichen Besitzers erzeugen kann.

Auch bei Facebook gibt es also eine Möglichkeit, die Nachrichten zu manipulieren. Im Vergleich zur SMS oder E-Mail ist diese aber aufgrund der Serverspeicherung eher als geringer einzuschätzen, die Beweissicherung könnte aber problematisch sein.

5. WhatsApp

WhatsApp ist ein (nahezu kostenfreier) Telekommunikationsdienst zum Austausch von Textnachrichten, Bild-, Video- und Tondateien zwischen Benutzern von Mobilgeräten. Laut Herstellerangaben gab es im April 2015 weltweit bereits über 800 Millionen aktive Nutzer. Nicht verwunderlich ist daher, dass WhatsApp somit auch vielfach

in Gerichtsprozessen ein Thema wird. So werden – laut der italienischen Vereinigung der Scheidungsanwälte – in 40 % aller Scheidungsprozesse, denen Ehebruch zugrunde liegt, WhatsApp-Nachrichten als Beweismittel angeführt.[6] Auch in Österreich gibt es schon Gerichtsfälle mit WhatsApp-Hintergrund, wobei es sich dabei meist um die Verbreitung von pornografischen Inhalten gegen den Willen der Beteiligten handelt.[7]

Ähnlich wie bei SMS findet keine zentrale Speicherung statt, sondern die gesendeten und erhaltenen Nachrichten werden am Smartphone in einer Art lokalem Safe gespeichert (Datei mgstore.db). Diese Datei dient im Wesentlichen als Datenbank, die eigentlich vom Anwender verborgen sein sollte. Jedoch sind die Verschlüsselungskeys im Internet verfügbar.[8] Darauf aufbauend sind auch verschiedenste Apps, die den Inhalt dieser Datenbank entschlüsseln, – sogar kostenfrei – erhältlich. Anwendungen, die auch einen schreibenden Zugriff auf die Datenbank zulassen, konnte der Autor jedoch nicht finden. Jedoch sollte es für einen Experten, wenn auch wohl nur mit hohem Aufwand, möglich sein, unter Zuhilfenahme der Keys den Inhalt der Datenbank zu verändern und somit bestehende WhatsApp-Nachrichten zu manipulieren.

Von Interesse ist auch hier die Frage, ob es möglich ist, WhatsApp-Nachrichten unter falschem Account zu verschicken. Hier kann aber im Gegensatz zur SMS nicht so einfach eine andere Telefonnummer vorgetäuscht werden. Zwar gibt es auch hier angebotene Dienste, etwa http://www.fakewhatsapp.com, um diesen zu nutzen ist es aber notwendig, das WhatsApp-Passwort zu kennen.

Dieses Passwort ist aber kein Passwort, das der Benutzer selbst vergibt, sondern das bei der Anlage des WhatsApp-Accounts automatisch generiert und nur für den Datenaustausch zwischen App und Server verwendet wird. Für den Benutzer ist es üblicherweise nicht sichtbar und kann auch nicht erraten werden. Möglich wäre aber ein Abhören des Datenverkehrs, etwa durch eine sogenannte *Man-in-the-middle*-Attacke, wobei aber hier WhatsApp aktuell eine vollständige Verschlüsselung der Datenübertragung umsetzt, womit auch diese Manipulationsmöglichkeit in Zukunft wegfallen wird.

Es lässt sich daher betreffend WhatsApp-Nachrichten festhalten, dass auch diese manipuliert werden können, wobei dafür aber sicherlich Expertenwissen notwendig ist.

6. Zusammenfassung

Zusammenfassend kann festgehalten werden, dass elektronische Nachrichten teilweise einfach manipuliert werden können. Insbesondere bei SMS und E-Mails können leicht andere Absender vorgetäuscht werden. Auch bei Facebook und WhatsApp ist das prinzipiell möglich, wobei insbesondere sogenannte Fake-Profile und leicht zu erratende Passwörter bei Facebook genannt werden können. Eine nachträgliche Veränderung der Nachricht ist bei SMS, E-Mail und WhatsApp ebenso möglich, wobei es bei E-Mails durch das Textformat besonders einfach ist. Für SMS und insbesondere WhatsApp wird es hier sicherlich stark fortgeschrittene Kenntnisse benötigen. Dadurch, dass bei Facebook alles zentral gespeichert wird, ist hier eine Änderung der Nachricht durch den Empfänger nicht möglich. Je nachdem, welche Manipulation durchgeführt wurde, wird es möglich sein, diese festzustellen. Manche Manipulationen lassen sich aber auch durch forensische Untersuchungen nicht beweisen. Eine Garantie, dass bei Gericht vorgezeigte derartige elektronische Nachrichten also echt sind, ist auf keinen Fall gegeben.

Anmerkungen:

1 Vgl *Knasmüller*, Zur Echtheit und Manipulation von SMS, SV 2013/4, 196.

2 *RTR*, RTR Telekom Monitor 1/2015 (2015) 9, online abrufbar unter http://www.rtr.at/de/komp/TKMonitor_1_2015/TM1_2015.pdf.

3 ZB OGH 1. 4. 2014, 14 Os 19/14x; 27. 11. 2014, 9 ObA 111/14k.

4 *Facebook*, Datenanfragen von Österreich, online abrufbar unter http://govtrequests.facebook.com/country/Austria/2014-H2/.

5 *SplashData*, „123456" Maintains the Top Spot on SplashData's Annual „Worst Passwords" List (2015), online abrufbar unter http://splashdata.com/press/worst-passwords-of-2014.htm.

6 WhatsApp: Massenhafte Überwachung der Nutzer via Online-Status, c´t 2015/2, 17.

7 ZB OGH 3. 7. 2014, 12 Os 56/14y.

8 *Mimikama*, WhatsApp Verschlüsselungskey im Internet aufgetaucht. Kein Fake – aber auch keine Sensation (2014), online abrufbar unter http://www.mimikama.at/allgemein/whatsapp-verschlsselungskey-im-internet-aufgetaucht-kein-fake-aber-auch-keine-sensation/, abgerufen am 10. 5. 2015.

Korrespondenz:
Dr. Markus Knasmüller
Edelhof 45, 3350 Haag
E-Mail: markus@knasmueller.at
Internet: http://www.knasmueller.at