Ing. Mag. Horst Greifeneder
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik;
Computer-Forensik-Spezialist

Forensische Sicherstellung und Auswertung von Facebook-Beiträgen

1. Einleitung

Soziale Medien wie Facebook, WhatsApp oder Instagram ermöglichen ihren Benutzern, sich über das Internet zu vernetzen. Im Rahmen dieser Vernetzung können Benutzer über verschiedene Dienste untereinander kommunizieren, mediale Inhalte öffentlich, in einer Gemeinschaft oder in ausgewählten Benutzerkreisen austauschen.

Die zunehmende gesellschaftliche Bedeutung der sozialen Medien spiegelt sich unter andrem in steigenden Zahlen von Gerichtsverfahren wider, in denen Beiträge oder Kommentare in sozialen Medien eine beweisrelevante Rolle spielen.

Der vorliegende Artikel widmet sich den Möglichkeiten, einzelne Beiträge und Kommentare in Facebook zu erstellen, und erörtert grundlegende Methoden zur Sicherstellung von Beweismitteln.

2. Facebook-Beiträge

2.1. Allgemeines

Facebook verfügt über eine Reihe von Funktionen zur Information, Kommunikation und Interaktion mit anderen Benutzern, Seiten oder Gruppen.

Angemeldete Benutzer können im Rahmen ihres webbasierten Facebook-Kontos oder ihrer Facebook-App unterschiedliche Beiträge veröffentlichen, unter anderem Statusmeldungen erstellen, Kommentare hinterlassen oder Antworten auf Kommentare schreiben (siehe Abbildung 1).

2.2. Erstellen einer Statusmeldung

Benutzer können Statusmeldungen als Textbeiträge mit beigefügtem Foto oder Video entweder über die eigene Chronik oder den eigenen News-Feed posten.

Beiträge (Posts) können zudem mit Markierungen anderer Personen, Symbolen zur Befindlichkeit oder aktuellen Tätigkeit, Ortsangaben sowie Zeit- und Datumsangaben versehen werden.

Die Möglichkeit zum Posten in der Chronik eines anderen Facebook-Benutzers ist – abhängig von den Kontoeinstellungen des anderen Facebook-Benutzers – aber grundsätzlich gegeben.

2.3. Zielgruppen

Der Kontoinhaber kann beim Erstellen eines Beitrags zudem die Empfänger (Zielgruppe) eines Beitrags gezielt auswählen und für einen bestimmten Beitrag auch nachträglich ändern.[1]

In der Regel stehen nachfolgende Optionen für die Zielgruppenauswahl zur Verfügung:[2]

- **Öffentlich:** Wird ein Beitrag vom Benutzer öffentlich geteilt, dann kann jeder Internetnutzer den Beitrag sehen, egal, ob er Facebook-Mitglied ist oder nicht.
- **Freunde (und Freunde von markierten Personen):** Mit dieser Option können Postings mit Facebook-Freunden geteilt werden. Werden andere Personen in einem Beitrag markiert, dann umfasst die Zielgruppe dieses Beitrags auch die markierte Person und deren Freunde.[3]
- **Nur ich:** Diese Option ermöglicht das Posten von Inhalten ausschließlich in der eigenen Chronik. Der Beitrag ist somit nur für den Beitragsersteller sichtbar.
- **Benutzerdefiniert:** Durch die Auswahl einer benutzerdefinierten Zielgruppe kann ein Posting nur mit bestimmten Personen geteilt oder vor bestimmten Personen verborgen werden. Außerdem können über benutzerdefinierte Einstellungen einzelne Beiträge auch nur mit bestimmten, vorher festgelegten Freundeslisten geteilt werden (wie zB mit der Familie oder den besten Freunden). Die benutzerdefinierte Auswahl der Zielgruppe ermöglicht es dem Beitragsersteller auch, einen Beitrag mit Facebook-Gruppen oder Netzwerken zu teilen, deren Mitglied er ist.[4]

Die Bestimmung der Zielgruppe (das ist die Menge der erreichten Personen) kann im Rahmen einer Befundaufnahme (zB zur rechtlichen Einordnung eines Delikts) erforderlich sein. Aus forensischer Sicht ist bemerkenswert, dass bei einem Posting nur die aktuelle Zielgruppenauswahl feststellbar ist. Eine nachträgliche Änderung der Zielgruppenauswahl ist weder im Beitrag noch aus dem Aktivitätenprotokoll ersichtlich.

2.4. Facebook-Kommentare

Bei einem Facebook-Kommentar handelt es sich um eine Text-, Bild oder Videonotiz zu einem bestehenden Beitrag.

Im Gegensatz zum Posting ist hier für den Ersteller des Kommentars keine Zielgruppenauswahl möglich.

3. Sicherstellung von Beweismitteln

3.1. Vorbemerkung

Bei der forensischen Sicherstellung von Beweismitteln im Zusammenhang mit strittigen Aktivitäten von Facebook-Nutzern (zB Hasspostings, Wiederbetätigung und Ähnliches) stehen dem Sachverständigen mehrere Beweismittelquellen und Methoden zur Verfügung:

- Erstellung eines Screenshots mit dem inkriminierten Beitrag bzw Kommentar;
- Sicherstellung von online verfügbaren Kontodaten;
- Gewinnung von lokal gespeicherten Facebook-Daten;
- Auskunftsansuchen zur Bekanntgabe von Benutzerdaten bei Facebook.

3.2. Screenshot des inkriminierten Beitrags bzw Kommentars

Die gängigste Methode ein Facebook-Posting sicherzustellen, ist die Anfertigung eines Screenshots.

Abbildung 1: Bildschirmausschnitt eines Facebook-Beitrags mit Foto, ohne zusätzliche Angaben

Unter einem Screenshot versteht man aus informationstechnischer Sicht das gesamte oder teilweise Erfassen des aktuellen Bildschirminhalts (zB einer Website) mit einer Betriebssystemfunktion oder einem anderen Programm mit entsprechender Screenshot-Funktion.

PC- oder Smartphone-Betriebssysteme wie Windows, iOS oder Android speichern einen Screenshot in der Regel über eine Taste oder Tastenkombination. Dabei wird ein Abbild des gesamten Bildschirminhalts in die Zwischenablage gelegt oder gespeichert. Von der Zwischenablage oder vom Speicherplatz kann der Screenshot in ein weiteres Programm (zB in ein Bildverarbeitungsprogramm) übernommen, gegebenenfalls weiterbearbeitet oder als Dokument gedruckt werden.

Manche Bildbearbeitungsprogramme oder Spezialprogramme bieten darüber hinaus erweiterte Funktionen zur Erstellung und Bearbeitung von Screenshots.

Beim Speichern des Screenshots als Bilddatei wird unter anderem das Erstelldatum der Datei gespeichert.

Aus computerforensischer Sicht sollte ein als Beweismittel vorgelegter Screenshot nachfolgende Informationen beinhalten und folgenden Anforderungen genügen:

- Abbildung des Bildschirms in seiner Gesamtheit;
- vollständige URL der aufgerufenen Seite;
- Zeitpunkt der Erstellung des Screenshots;
- Name des Erstellers;
- Angabe der Bildschirmauflösung;
- Informationen zum Betriebssystem, Browser, Screenshot-Tool usw;
- Tab-Inhalt bzw Title-Tag der Seite;
- Verfügbarkeit des Screenshots im Original als Bilddatei;
- Hash der Screenshot-Bilddatei;
- Dokumentation des Quelltextes der dokumentierten Seite;
- Einhaltung des Vieraugenprinzips.

Je mehr der angeführten Informationen verfügbar bzw je mehr dieser Anforderungen erfüllt sind, desto höher ist die Aussagekraft eines als Beweismittel sichergestellten Screenshots.

3.3. Online verfügbare Kontodaten des Benutzers

3.3.1. Allgemeines

Eine weitere Methode zur Sicherstellung von Beweismitteln im Zusammenhang mit strittigen Facebook-Aktivitäten eines Nutzers erfordert die Zugangsdaten zu dessen Facebook-Konto.

Über den Zugang zu den im Konto gespeicherten Daten stehen dem Sachverständigen für die Befundaufnahme das Aktivitätenprotokoll bzw die Archivdatei als Beweismittelquellen zur Verfügung.

3.3.2. Aktivitätenprotokoll

Das Aktivitätenprotokoll ist eine Liste von benutzerbezogenen Beiträge und Aktivitäten seit der erstmaligen Nutzung von Facebook (siehe Abbildung 2).[5] Das Aktivitätenprotokoll enthält benutzerbezogene Meldungen, geordnet nach dem Ereignistag auf Facebook. Meldungen aus dem Aktivitätenprotokoll können an anderen Orten auf Facebook erscheinen (beispielsweise in der benutzerbezogenen Chronik, in der Suche oder im News-Feed der Freunde des Benutzers).

Abbildung 2: Bildschirmausschnitt des Aktivitätenprotokolls

Das Aktivitätenprotokoll kann vom angemeldeten Benutzer jederzeit abgerufen werden. Über das Aktivitätenprotokoll können auch Meldungen vom Benutzer gelöscht oder in seiner Chronik verborgen werden.

3.3.3. Facebook-Archivdatei

Facebook bietet dem Kontoinhaber bzw einem im Besitz der gültigen Zugangsdaten befindlichen Benutzer die Möglichkeit, eine Kopie der auf Facebook gespeicherten persönlichen Daten als Archivdatei herunterzuladen. Es ist nicht möglich, individuell festzulegen, welche Daten beim Herunterladen der Facebook-Informationen bezogen werden, das heißt, die Datei wird vollständig heruntergeladen.[6]

Die Download-Datei enthält ein HTML-basiertes Facebook-Archiv, welches dennoch nur einen Teil der Informationen, die bei Facebook über ein benutzerbezogenes Konto zur Verfügung stehen, enthält (siehe Abbildung 3).[7]

Informationen und Inhalte, die vom Benutzer gelöscht wurden, sind laut Facebook nicht verfügbar, da diese von den Facebook-Servern gelöscht werden.

Welche Information ist verfügbar?	Was ist das?	Wo kann ich es finden?
Profil- und Kontakt-informationen	Name, E-Mail-Adresse, Registrierungsdatum, frühere Profilnamen, Seiten, Gruppen, Adressbuch uvm.	Archivdatei
Über mich	Informationen, die der Benutzer unter dem „Über"-Bereich in seiner Chronik hinzugefügt hat (wie Beziehungen, Arbeit, Bildung, wo der Benutzer lebst und mehr). Dies beinhaltet alle Aktualisierungen und Änderungen, die der Benutzer in der Vergangenheit vorgenommen hat, und alle Informationen, die momentan im „Info"-Bereich deiner Chronik zu finden sind.	Aktivitätenprotokoll Archivdatei
Beiträge für andere	Alles, was der Benutzer bei jemand anderem in der Chronik gepostet hat (wie Fotos, Videos und Statusmeldungen).	Aktivitätenprotokoll
Beiträge von anderen	Alles, was andere Nutzer in der Chronik des Benutzers posten (etwa Pinnwandeinträge oder von Freunden geteilte Links).	Aktivitätenprotokoll Archivdatei
Beiträge von dir	Alle Beiträge des Benutzers (wie Fotos, Videos, Statusmeldungen), die der Benutzer in seiner eigenen Chronik gepostet hat.	Aktivitätenprotokoll Archivdatei
Fotos	Fotos, die der Benutzer auf sein Konto hochgeladen hat, inklusive einer Fülle von Foto-Metadaten, die mit den vom Benutzer hochgeladenen Fotos übermittelt werden.	Archivdatei
Freunde	Liste der aktiven und gelöschten Freunde sowie versandte und empfangene Freundschaftsanfragen.	Archivdatei
Nachrichten	Nachrichten, die der Benutzer auf Facebook gesendet und empfangen hast. Zu beachten ist, dass gelöschte Nachrichten nicht in dem Download enthalten sind, da diese aus dem Konto gelöscht wurden.	Archivdatei
Sicherheitsinformationen, An- und Abmeldungen, Verwaltungsunterlagen	IP-Adresse, Datum und Zeit in Verbindung mit Kontoaktivitäten (wie An- und Abmeldungen sowie Passwortänderungen).	Archivdatei

Abbildung 3: Verfügbare Daten in der Archivdatei und/oder im Aktivitätenprotokoll

3.4. Gewinnung von lokal gespeicherten Facebook-Daten

3.4.1. Allgemeines

Auf persistenten Speichermedien (zB Festplatten) finden sich Spuren von Facebook-Aktivitäten (etwa von Postings oder Kommentaren) als Artefakte gängiger Webstandardformate (wie HTML, JSON oder Ähnliches) sowohl in allokierten als auch unallokierten Speicherplätzen wieder.

Die gegebenenfalls verfügbaren Beweise sind unter anderem abhängig vom vorhandenen Betriebssystem und der verwendeten Software zur Erstellung von Facebook-Postings.

Die forensische Sicherstellung der Artefakte erfolgt in der Regel durch die Auswertung (Carven) von Speicherplätzen für temporäre Internetdateien (Cache) und Arbeitsspeicher-Dumps.[8]

Nahezu alle gängigen forensischen Softwarepakete (wie EnCase, FTK oder Magnet IEF) unterstützen die Sicherstellung von Facebook-Artefakten am Computer oder Smartphone. Da die Betreiber von Social-Media-Plattformen wie Facebook immer wieder die Protokolle, Speicherorte bzw Sicherheitsstandards ihrer Anwendungen verändern, empfiehlt sich bei der Sicherstellung von Beweismitteln für benutzerspezifische Facebook-Aktivitäten die Nutzung verschiedener Werkzeuge, um die Menge der sichergestellten Daten zu erhöhen sowie deren Beweiskraft zu stärken.[9]

Weitere Hinweise im Zusammenhang mit Facebook-Postings liefern Bilder oder URLs.

3.4.2. Facebook-Bilder

Ein weiteres aus forensischer Sicht interessantes Beweismittel im Zusammenhang mit Facebook-Aktivitäten von Benutzern sind auf Facebook gepostete Bilder. Auf Facebook veröffentlichte Bilder verfügen in der Regel über ein charakteristisches Dateinamenmuster, wonach auf Speichermedien gezielt gesucht werden kann.

Facebook nutzt eine kleine Anzahl unterschiedlicher Dateinamenstrukturen zur Benennung von Bildern. Der Name einer Bilddatei besteht in der Regel aus drei mit Unterstrichen getrennten Ziffernfolgen (zB 12265655_10102475457180761_7081554074581754773_o.jpg) und offenbart unter anderem Informationen zum Kontoinhaber.

So liefert die zweite Nummernfolge im Dateinamen einen Hinweis auf die Photo-ID des Bildes. Bei Eingabe des Links http://www.facebook.com/10102475457180761 im Browser wird direkt das damit verknüpfte Bild aufgerufen. Über das gezeigte Bild ist es dann auch möglich, den Kontoinhaber zu eruieren.

3.5. Auskunft über Benutzerdaten bei Facebook

Facebook bietet für autorisierte Richter, Staatsanwälte sowie sonstige Strafverfolgungsbehörden im Rahmen von offiziellen Ermittlungen die Möglichkeit, in Übereinstimmung mit den eigenen Geschäftsbedingungen und dem anwendbaren Recht online eine Anfrage zu Daten von Benutzerkonten durchzuführen.[10]

Anmerkungen:

1 Wie wähle ich beim Posten eines Beitrags, wer diesen Beitrag sehen kann?, online abrufbar unter https://www.facebook.com/help/120939471321735.

2 Welche Zielgruppen kann ich beim Teilen von Inhalten auswählen?, online abrufbar unter https://www.facebook.com/help/211513702214269.

3 Möchte der Benutzer vermeiden, dass sein Beitrag für Freunde der von ihm markierten Personen sichtbar ist, kann er diese Grundeinstellung über die Zielgruppenauswahl entfernen.

4 Facebook-Gruppen und Netzwerke sind öffentliche oder geschlossene Benutzerkreise. Während der Benutzer eine Facebook-Gruppe selbst erstellen und verwalten kann, werden Netzwerke von Dritten erstellt und verwaltet und sind nur für deren Mitglieder zugänglich.

5 Mehr über das Aktivitätenprotokoll erfahren, online abrufbar unter https://www.facebook.com/help/437430672945092.

6 Deine Informationen herunterladen, online abrufbar unter https://www.facebook.com/help/131112897028467.

7 Die Betreiber der Website http://europe-v-facebook.org weisen darauf hin, dass in den Datensätzen viele Informationen fehlen und Facebook in Wirklichkeit noch mehr Daten speichert; siehe http://europe-v-facebook.org/DE/Datenbestand/datenbestand.html.

8 How important are Facebook Artifacts? (2013), online abrufbar unter https://www.magnetforensics.com/computer-forensics/how-important-are-facebook-artifacts/.

9 *Mahalik/Tamma/Bommisetty*, Practical Mobile Forensics[2] (2016) 349.

10 Law Enforcement Online Requests, online abrufbar unter https://www.facebook.com/records/x/login.

Korrespondenz:
Ing. Mag. Horst Greifeneder
Schenkelbachweg 32, 4600 Wels
Tel.: 07242 / 77715
Fax: 07242 / 77716
E-Mail: office@fds.at