MARKTWÄCHTER
DIGITALE WELT

verbraucherzentrale

DER UNBEKANNTE DRITTE

Drittanbieter am deutschen Mobilfunkmarkt

Eine Untersuchung der Verbraucherzentralen – September 2017

DER UNBEKANNTE DRITTE

1. EINLEITUNG UND ZIELSETZUNG 5

2. UNTERSUCHUNGSGEGENSTAND 8
2.1 Hintergrund des Bezahlverfahrens und Marktentwicklung 8
2.2 Ausprägungen & Ablauf des Bezahlverfahrens 9
2.3 Angriffstechnik und Verbreitung 11
2.4 Darstellung auf der Telefonrechnung 12

3. DRITTANBIETERPROBLEMATIK AUS VERBRAUCHERSICHT 14
3.1 Frühwarnnetzwerk 14
3.2 Ausprägungen in der Bevölkerung – repräsentative Umfrage 18
3.3 Zusammenfassung – Drittanbieterproblematik aus Verbrauchersicht 23

4. DRITTANBIETERMARKT UND SICHERUNGSMECHANISMEN 25
4.1 Akteure im Drittanbietermarkt 25
4.2 Die Clean Market Initiative der Mobilfunkunternehmen 27
4.3 Redirect 29
4.4 Zusammenfassung Drittanbietermarkt und Sicherungsmechanismen 31

5. RECHTLICHE ANALYSE DER DRITTANBIETERPROBLEMATIK 33
5.1 Allgemeine rechtliche Aspekte 33
5.2 Voreingestellte Drittanbietersperre 35
5.3 Gesamtrechnung 36
5.4 Die Redirect-Bezahlseite 36
5.5 Zusammenfassung der rechtlichen Analyse 37

6. MISSBRAUCHSSZENARIEN UND REDIRECT – UNTERSUCHUNG FRAUNHOFER INSTITUT 38
6.1 Missbrauchsszenarien mittels Webbrowser 38
6.2 Missbrauchsszenarien mittels Smartphone-Applikation 41
6.3 Zusammenfassung der Überprüfung von Missbrauchsszenarien und Redirect-Verfahren 42

7. FAZIT UND SCHLUSSFOLGERUNGEN 43

LITERATURVERZEICHNIS 48

ABKÜRZUNGSVERZEICHNIS 55

GLOSSAR 57

ABBILDUNGEN UND TABELLEN

1 Methodisches Vorgehen 7

2 Digitaler Content monetarisiert durch Carrier Billing in Europa nach Region 9

3 Beispiele für Bestellungen von Drittanbieterleistungen 10

4 Schema zum Angriffsvektor Clickjacking 11

5 Versand einer SMS-Bestätigung nach Kauf einer Drittanbieterleistung 11

6 Musterrechnung O2 – Rechnungsdetails 13

7 Bezahlen von Drittanbieterleistungen über die Mobilfunkrechnung 20

8 Verteilung absichtlicher und unabsichtlicher Abschluss von Drittanbieterleistungen 20

9 Bezahlen von Drittanbieterleistungen über die Mobilfunkrechnung nach Abschlussart 21

10 Häufigkeitsverteilung der Vertragsarten 22

11 Häufigkeitsverteilung der Überprüfung der Mobilfunkrechnung 22

12 Gründe für das Nicht-Prüfen der Mobilfunkrechnung 23

13 Schadenssummen durch unabsichtlichen Abschluss von Drittanbieterleistungen 24

14 Akteure im Drittanbietermarkt 25

15 Einheitlicher Bezahlprozess der Clean-Market Initiative 27

16 Redirect-Bezahlseiten im Vergleich (Stand: 2016) 30

17 Technisch flächendeckend möglicher Einsatz des Redirect Verfahrens 30

18 Beispielhafte Darstellung eines CAPTCHAs 39

19 Redirect-Bezahlseiten mit Sicherungsmechanismen (Stand: 2017) 40

1. EINLEITUNG UND ZIELSETZUNG

Ende der 90er-Jahre gelang der Mobiltelefonie der endgültige Durchbruch in Deutschland. Bereits damals war es möglich, sein Handy mit Bildschirmhintergründen und Klingeltönen zu individualisieren. Eines der am weitverbreitetsten Angebote war der „Crazy Frog“ des Unternehmens Jamba. Man bestellte den Klingelton per SMS und hatte in vielen Fällen ein Abo abgeschlossen, das einem jede Woche einen neuen Klingelton lieferte. Bezahlt wurde über die Telefonrechnung.

Mehr als zehn Jahre später ist der Frosch zwar aus den Lautsprechern der Mobilfunktelefone verschwunden, der Markt für das Bezahlen über die Mobilfunkrechnung ist allerdings geblieben – und hat eine immense Entwicklung genommen. Nicht ausschließlich zum Vorteil der Verbraucher, wie die Zahl an Beschwerdefällen in den Beratungsstellen der Verbraucherzentralen dokumentiert. In den Jahren 2014 bis 2016 tappten Verbraucher immer öfter über das als WAP-Billing (Wireless Application Protocol) bekannte Verfahren in Abofallen. Über ihre Handyrechnung bekamen sie also Posten von Dritten verbucht, welche sie gar nicht bestellt hatten. Allein im Frühwarnnetzwerk (FWN)[1], einem Erfassungs- und Analysesystem für auffällige Sachverhalte aus der Verbraucherberatung, stellen Probleme mit Drittanbieterkosten seit Ende 2015 den häufigsten Beschwerdegrund für Verbraucher im Telekommunikationsmarkt dar.

Besonders an dieser Thematik ist, dass die Verbraucher oftmals nicht nachvollziehen können, wie der als Leistungen Dritter titulierte Posten auf ihre Rechnung gelangt ist. Ebenso sind dem Verbraucher die in der Rechnung genannten Unternehmen meistens unbekannt. Die aufgeführten Beträge werden automatisch durch die Telekommunikationsanbieter eingezogen und sind – wenn überhaupt – nur mit erheblichem Aufwand wiederzubekommen.

Dabei ist das Thema Abofallen im Mobilfunk kein neues. Bereits in den Jahren 2010/11[2] waren die Verbraucherzentralen in Deutschland intensiv mit diesem Sachverhalt beschäftigt. Dies mündete letztlich in der Forderung des Verbraucherzentrale Bundesverbandes (vzbv) nach einer voreingestellten Drittanbietersperre, die Mobilfunkkunden vor einer unbeabsichtigten Abbuchung schützt. Im Rahmen der TKG-Novelle 2012 wurde diese Forderung vom Gesetzgeber jedoch nicht umgesetzt.

Am 27. April 2017 hat der Bundestag nun der Bundesnetzagentur den Auftrag erteilt, ein Verfahren festzulegen, das „den Teilnehmer wirksam davor schützen (soll), dass eine neben der Verbindung erbrachte Leistung gegen seinen Willen in Anspruch genommen und abgerechnet wird.“[3]

Fragen und Struktur

Ziel der vorliegenden Untersuchung ist es, eine umfassende Betrachtung der Drittanbieterproblematik aus unterschiedlichen Blickwinkeln zu ermöglichen und damit die Fragen zu klären, warum derartige Fälle immer wieder auftauchen und in welcher Höhe auftretende Schäden einzuschätzen sind.

Ausgehend von einer Beschreibung des Untersuchungsgegenstandes (Kapitel 2), wird in Kapitel 3 das Problemfeld aus Verbrauchersicht betrachtet. Dazu wird die Situation anhand von Sachverhalten aus den Beratungsstellen der Verbraucherzentralen dargestellt (Kapitel 3.1). Die Perspektive wird durch eine repräsentative Befragung der deutschen Mobilfunknutzer erweitert (Kapitel 3.2). In Kapitel 4 erfolgt eine Analyse der aktuellen, segmentspezifischen Marktsituation für mobile Bezahlverfahren (Kapitel 4.1), in der auch die Aktivitäten vor allem der Netzbetreiber zu dem hier untersuchten Thema abgebildet werden (Kapitel 4.2 und 4.3). Daran schließt mit Kapitel 5 die rechtliche Ausarbeitung zur Drittanbieterproblematik an, bevor in Kapitel 6 die technische Dimension beleuchtet wird. Kapitel 7 interpretiert die Resultate und gibt einen allgemeinen Ausblick auf die Thematik.

Um den Sachverhalt der ungewollten Rechnungsstellung von Drittanbietern aus allen Perspektiven zu beleuchten, wird als Untersuchungsmethode auf den Mixed-Methods-Ansatz[4] zurückgegriffen. Dieser ist für die

1 Für eine genauere Beschreibung des FWNs siehe Kapitel 3.1.1.
2 Vgl. Bleich (2011).
3 Deutscher Bundestag (2017).
4 Auch als Methoden-Triangulation bekannt.

vorliegende Studie als geeigneter Ansatz identifiziert worden, da er ein größeres und komplexeres Verständnis des Untersuchungsgegenstandes ermöglicht.[5] Die Ergebnisse der einzelnen Untersuchungsbereiche stehen dabei nicht unabhängig nebeneinander, sondern beziehen sich vielmehr direkt aufeinander.

Eine Gesamtübersicht über das methodische Vorgehen zeigt das nachfolgende Schaubild (Abbildung 1), an das die Forschungsfragen anschließen, die im Rahmen dieser Untersuchung beantwortet werden. Eine detaillierte Beschreibung der einzelnen Ansätze findet sich in den jeweiligen Untersuchungsabschnitten.

Die vorliegende Untersuchung wurde zwischen dem 12.05.2016 und dem 19.01.2017 durchgeführt, zudem wurden einige Aspekte im Laufe des Jahres 2017 erneut geprüft.

Im Vorfeld der Hauptuntersuchung wurde die Expertise der Telekommunikations-Spezialisten der Verbraucherzentralen in die Entwicklung des Fragebogens für die bevölkerungsrepräsentative Umfrage eingebunden.

Darüber hinaus wurden im Rahmen eines Expertengespräches erste Erkenntnisse mit folgenden Institutionen und Unternehmen diskutiert:

- Bundesnetzagentur
- Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V. (VATM)
- Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
- mobilsicher.de
- Deutsche Telekom AG/Telekom Deutschland GmbH
- Telefónica Germany GmbH & Co. OHG
- Vodafone GmbH
- freenet AG/mobilcom-debitel GmbH
- mbe GmbH
- Verbraucherzentrale Brandenburg e. V.
- Verbraucherzentrale Hamburg e. V.
- Verbraucherzentrale Niedersachsen e. V.
- Verbraucherzentrale Nordrhein-Westfalen e. V.
- Verbraucherzentrale Rheinland-Pfalz e. V.
- Verbraucherzentrale Sachsen e. V.
- Verbraucherzentrale Schleswig-Holstein e. V.
- Verbraucherzentrale Bundesverband e. V.

5 Vgl. Creswell (2008).

? DIE FOLGENDEN GRUNDLEGENDEN FRAGEN WERDEN IM RAHMEN DIESER UNTERSUCHUNG BEANTWORTET

Forschungsfrage 1
Um welches Bezahlverfahren geht es?

Forschungsfrage 2
Wie funktioniert das Bezahlverfahren?

Forschungsfrage 3
Wie stellt sich das Problem in den Verbraucherzentralen dar?

Forschungsfrage 4
Welche Relevanz besitzt das Problem in der Bevölkerung?

Forschungsfrage 5
Welche technischen und organisatorischen Aspekte müssen für dieses Verfahren berücksichtigt werden?

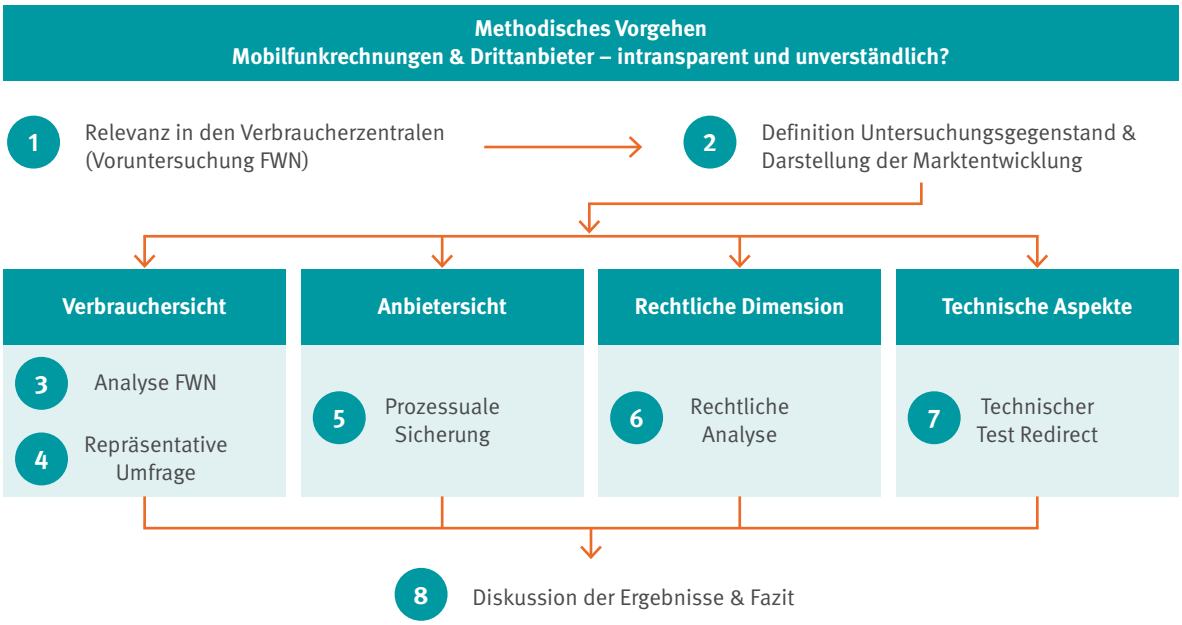
Forschungsfrage 6
Wie gestaltet sich die Drittanbieterproblematik in rechtlicher Hinsicht?

Forschungsfrage 7
Welche Schutzmechanismen wurden eingeführt und sind diese ausreichend?

Für weitere Hintergrundinformationen und Anfragen bestand zudem Kontakt zur Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Abteilung Erlaubnispflicht und Verfolgung unerlaubter Geschäfte, sowie zur mdk Gesellschaft für Entwicklung und Betrieb technischer Mehrwertdiensteplattformen mbH, die im Auftrag der Mobilfunknetzbetreiber[6] ein Kontrollverfahren im Rahmen der Drittanbieterabrechnungen durchführt.

6 Das sind in Deutschland die Unternehmen Telefónica Germany, Telekom Deutschland und Vodafone.

1 METHODISCHES VORGEHEN



Begriffsdefinition

Die Analyse von Beschwerdefällen aus den Verbraucherzentralen zeigte bereits im Vorfeld der Untersuchung einen deutlichen Schwerpunkt von strittigen Drittanbieterfällen, die dem WAP- bzw. Direct Billing-Verfahren zuzuordnen sind, so dass im Rahmen dieser Studie diese Variante genauer betrachtet wird. Um dieses Verfahren von anderen abzugrenzen, erscheint im Vorwege jedoch eine Begriffsdefinition notwendig:

Übergeordnet umschreibt das **Geschäftsmodell** Carrier Billing[7] die Berechnung bestimmter Transaktionen, die in der Regel mit dem Mobiltelefon durchgeführt und über die Rechnung des Mobilfunkunternehmens abgebucht wurden. Im Folgenden soll der Begriff **Carrier Billing** verwendet werden, wenn inhaltlich auf das Geschäftsmodell im Allgemeinen Bezug genommen wird.

In dem Geschäftsmodell Carrier Billing sind mehrere Ausprägungen der **technischen Umsetzung** enthalten, die der Verbraucher im Rahmen seiner Nutzung wahrnehmen kann. Bei allen Varianten handelt es sich dabei zuerst um ein elektronisches Bezahlverfahren, das in der Regel **nicht** am Point of Sale (POS) im Ladengeschäft eingesetzt wird,[8] sondern in räumlicher Entfernung, sozusagen als Fernzahlungsmethode oder -möglichkeit (Remote Payment).[9]

Von besonderem Interesse in der technischen Umsetzung ist das **WAP-Billing** bzw. besser **Direct Billing**[10]. In dieser Studie soll von **Direct Billing** gesprochen werden, wenn es um die konkrete technische Ausgestaltung dieses Bezahlverfahrens während einer mobilen Internetsitzung geht, unabhängig davon, ob dieses Verfahren direkt über eine Webseite des Browsers oder eine App auf dem Smartphone in Anspruch genommen wird.

7 Alternativ auch Direct Operator Billing, Mobile Operator Billing, Mobile Operator Payment oder auch nur Operator Billing genannt.

8 Wie zum Beispiel Verfahren im Zusammenhang mit der NFC-Technologie.

9 Siehe zum Beispiel Juniper Research/Dimoco (2013), S. 7.

10 Direct Billing ist als beschreibender Begriff geeigneter, da er unabhängig vom eingesetzten technischen Standard verwendet werden kann.

2. UNTERSUCHUNGSGEGENSTAND

2.1 HINTERGRUND DES BEZAHLVERFAHRENS UND MARKTENTWICKLUNG

Als digitales Zahlungsverfahren geht das Carrier Billing auf die Anfänge des Mobile Payment zurück. Der Begriff selbst umschreibt die Berechnung bestimmter Transaktionen, die meist mit dem Mobiltelefon durchgeführt und über die Rechnung des Mobilfunkanbieters abgebucht werden. Damit sind Electronic Payment Systeme angesprochen, die Böhle[11] in drei Kategorien unterscheidet: 1. Access Products, also Verfügungsinstrumente über Bankkonten, 2. Prepaid Products, also vorausbezahlte Verfahren und 3. Inkassosysteme, wozu auch das Carrier Billing gehört.

Da inkassobasierte Systeme oftmals auf bestehende Rechnungsbeziehungen aufsetzen, können hierbei hohe Komplexität und Kosten vermieden werden.[12] Nicht zuletzt deswegen eignet sich dieses Bezahlverfahren insbesondere für die Vermarktung digitaler Inhalte im Micropayment-Bereich, also Segmenten, in denen es um Kleinstbeträge geht.

Zu diesen Kleinstbeträgen zählen auch monatliche oder wöchentliche Abonnements über Klingeltöne oder sonstige digitale Serviceleistungen, welche seit Beginn der jüngsten Jahrtausendwende zunehmend stark genutzt werden. Besonders interessant ist die Zahlung durch Carrier Billing vor allem für Jugendliche, also eine Zielgruppe, die aufgrund ihres Alters keinen Zugang zu Bankkonten oder Kreditkarten hat.[13]

Dabei ist Carrier Billing via Mobilfunkunternehmen keinesfalls auf digitale Güter beschränkt, wie M-Pesa, ein Joint-Venture von Vodafone und dem afrikanischen Mobilfunkanbieter Safari.com zeigt. Vor allem in Ländern ohne etablierte Banksysteme kann ein bargeldloser Zahlungsverkehr über das Mobiltelefon eine ernsthafte Alternative zu Bankdienstleistungen darstellen.[14]

Pilotprojekte der Telekommunikationsunternehmen, mobile Bezahlverfahren, beispielsweise mpass oder NFC City Berlin, auch im deutschsprachigen Raum zu positionieren, wurden aktuell wieder eingestellt.[15] Laut der Studie „Interaktiver Handel in Deutschland – Ergebnisse 2015“ des behv liegt die Nutzung des Bezahlweges über die Telefonrechnung mit sechs Prozent deutlich hinter anderen, wie zum Beispiel per Kreditkarte mit 41 Prozent oder per Bankeinzug mit 27 Prozent.[16] Diese niedrige Nachfrage könnte sowohl auf ein mangelndes Vertrauen in die Telekommunikationsunternehmen als Payment-Service-Provider[17] als auch auf den fehlenden Bedarf (insbesondere im stationären Handel) zurückgeführt werden.[18]

Dass Carrier Billing dennoch ein großes Potenzial mitbringt, ergibt sich aus der Tatsache, dass mobile Endgeräte deutlich stärker verbreitet sind als beispielsweise Debit- und Kreditkarten.[19] Hinzu kommt, dass sich in den vergangenen Jahren die Möglichkeiten, digitale Inhalte zu erwerben und zu nutzen, deutlich verändert haben. So beschreibt der Begriff der sogenannten Subscription Economy[20] einen aktuellen Trend hin zur Nutzung von Abonnements. Diese können für einen Zeitraum individuell gebucht und genutzt werden. Zu den erfolgreichsten Anbietern solcher Abonnements zählen beispielsweise Netflix, Amazon und Spotify[21], aber auch im Spielebereich ist diese Entwicklung zu beobachten, wie aktuelle Marktdaten belegen.[22]

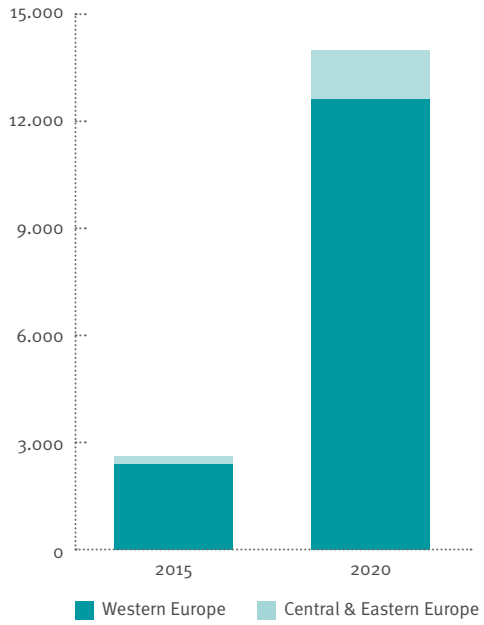
Branchenstudien messen aber der Entwicklung digitaler Inhalte das größte wirtschaftliche Potential bei, insbesondere da diese Dienste über immer mehr Endgeräte, wie beispielsweise den heimischen Smart-TV oder zukünftig auch das vernetzte Auto, genutzt werden können.[23]

In einer Analyse[24] geht Juniper Research davon aus, dass die Einnahmen aus dem Verkauf digitaler Inhalte über dieses Geschäftsmodell europaweit von 2,6 Milliarden

11 Vgl. Böhle (2002).
12 Vgl. Dannenberg (2004).
13 Vgl. Hernandez (2014) und Krüger (2016), S. 217.
14 Vgl. Krüger (2016), S. 221 ff.
15 Vgl. Krüger (2016) S. 228 ff.
16 Siehe Bundesverband E-Commerce und Versandhandel e. V. (2016), S. 30.
17 Vgl. Klees et al. (2013).
18 Siehe z. B. Scholz (2016).
19 Vgl. Juniper Research/Dimoco (2016), S. 14.
20 Siehe z. B. Empson (2013) oder Zuora Inc. (2017).
21 Siehe z. B. Goldmedia GmbH (2016).
22 Siehe Bundesverband Interaktive Unterhaltungssoftware e. V. (2016).
23 Vgl. Juniper Research/Dimoco (2016), S. 16 ff.
24 Vgl. ebda.

2 DIGITALER CONTENT MONETARISIERT DURCH CARRIER BILLING IN EUROPA NACH REGION

European Digital Content Revenues Monetised Through Carrier Billing, By Sub-Region, 2015 & 2020 (€m)



	2015	2020
Western Europe	2.397,80	12.616,60
Central & Eastern Europe	212,40	1.373,50
Total	**2.610,20**	**13.990,10**

Quelle: Juniper Research/Dimoco (2016)

Euro in 2015 auf knapp 14 Milliarden EUR in 2020 anwachsen werden. Der Marktanteil des Carrier Billings am Gesamtumsatz digitaler Inhalte würde dabei von 9 Prozent auf 25 Prozent steigen.[25]

Ein wesentlicher Vorteil des Direct Billings liegt – im Vergleich zu anderen mobilen Bezahloptionen – in einer deutlich höheren Konversionsrate, also einem höheren Anteil von Nutzern, die zu zahlenden Kunden werden, sowie in zum Teil niedrigeren Transaktionskosten.[26] Diese beiden Aspekte sind gerade für Händler interessant, um ihre Produkte erfolgreich am Markt zu positionieren. Für Anbieter digitaler Inhalte, häufig sogenannte OTT-Dienste[27], ist Carrier Billing von Interesse, weil es auf bereits bestehende Verträge aufbaut – und das Bezahlverfahren somit für Nutzer recht einfach zu handhaben ist. Auch die Netzbetreiber können dann Vorteile aus diesem wachsenden Markt ziehen, da sie an den Absätzen der gekauften Leistungen prozentual beteiligt sind.[28]

25 Ebda., S. 26 ff.
26 Vgl. Abraham und van der Lande (2013).
27 Over-The-Top Dienste, in diesem Fall Dienste wie beispielsweise Spotify.
28 Vgl. ebda.

2.2 AUSPRÄGUNGEN & ABLAUF DES BEZAHLVERFAHRENS

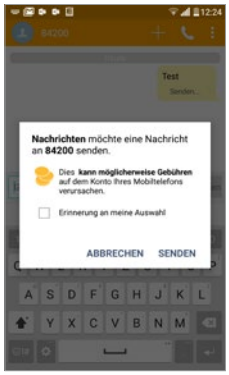
Im Rahmen des Carrier Billings haben Mobilfunkkunden verschiedene Möglichkeiten, Drittanbieterangebote zu bestellen, wie die folgenden, nicht abschließenden Beispiele zeigen.

Von besonderem Interesse für diese Studie ist der Abo-Abschluss über einen mobilen Internetzugang (siehe Beispiel b) in Abbildung 3). Je nach technischem Status des Endgerätes und verwendetem Browser werden dabei mobile Internetverbindungen als Standard-HTML-Sessions[29] oder bei älteren Geräten mit dem veralteten Wireless Application Protocoll (WAP) aufgebaut. Bei jedem Besuch einer Webseite, beziehungsweise bei jeder Internetsitzung, werden in Abhängigkeit des eingesetzten Protokolls[30] unterschiedliche Daten über den sogenannten Header an den Webseitenbetreiber mitgeliefert. Der Header kann dabei sinnbildlich als Kopf eines Da-

29 Kurz für Hypertext Markup Language (HTML).
30 WAP, IPv4 oder IPv6.

3 BEISPIELE FÜR BESTELLUNGEN VON DRITTANBIETERLEISTUNGEN

a **Via Bestell-SMS an eine Kurzwahlnummer**

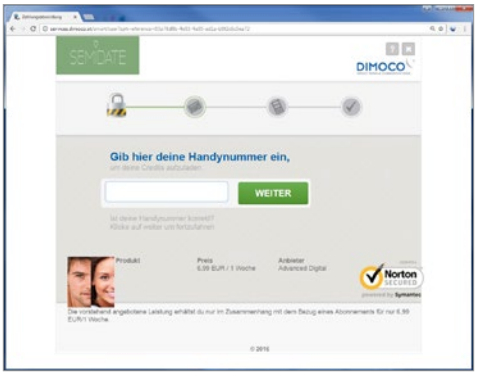


Screenshot (SMS-App) über ein LG G4

b **Bestellung über das mobile Internet**

http://playclub.io

c **Via Eingabe der MSISDN zum Abschluss eines Abos mit dem PC über das WLAN**



http://services.dimoco.at

Anm.: Die Darstellungen können zwischen den eingesetzten Endgeräten und den jeweiligen Angeboten variieren.

tenblocks angesehen werden, der Zusatzinformationen mitliefert.[31]

Um nun zu erkennen, welcher Nutzer ein Abonnement über die mobile Internetverbindung gebucht hat, ist die Übergabe eines Identifikationsmerkmals zum Vertragsschluss notwendig. Die während einer Internetsitzung übermittelte IP-Adresse reicht nicht aus, da sie lediglich Aufschluss über den Netzbetreiber[32], nicht aber über den Nutzer gibt. Zur Identifikation wird deshalb die MSISDN (Mobilfunkrufnummer) des Teilnehmers verwendet, die während des Vertragsschlusses an den Drittanbieter beziehungsweise den Aggregatoren übergeben wird. Der Aggregator, auch Enabler oder Billing-Carrier genannt, ist das Bindeglied zwischen Drittanbieter und Mobilfunkunternehmen und nimmt verschiedene Funktionen in diesem Prozess ein.[33] Diese MSISDN wird nicht in Klartext übertragen, kann aber nach Aussagen von Telekommunikationsunternehmen bei mobilen Internetsitzungen aus bestimmten Daten des Headers derzeit noch in die MSISDN transformiert werden.[34] Ob der Verbraucher dabei eine WAP-Seite oder eine HTML-Seite aufruft, ist für den Vertragsschluss unerheblich, da die zur Identifikation des Nutzers notwendigen Informationen in beiden Fällen übergeben wird. Zudem ist ein optischer Unterschied dieser beiden Seitentypen für den Anwender kaum auszumachen.

Wird ein Abonnement im Rahmen des Direct Billings abgeschlossen, dann soll der Verbraucher laut Netzbetreibern mindestens eine Bestätigungs-SMS erhalten. Einzig Vodafone gibt an, auch im Fall eines Einzelkaufes eine solche SMS zu versenden.[35]

Anders ist die Situation, wenn der Verbraucher die Webseite eines Drittanbieters aus einem WLAN heraus aufruft. In diesem Fall stehen die genannten Optionen zur Identifikation des Nutzers nicht zur Verfügung. Der Anbieter kann alternativ auf die einheitliche Bezahlmaske der Clean Market Initiative weiterleiten, in welche der Verbraucher seine MSISDN eingeben muss (siehe Beispiel c in Abbildung 3).

31 Zum Beispiel die IP-Adresse der Station, die das Datenpaket abgeschickt hat sowie die IP-Adresse der Station, für die das Paket bestimmt ist.

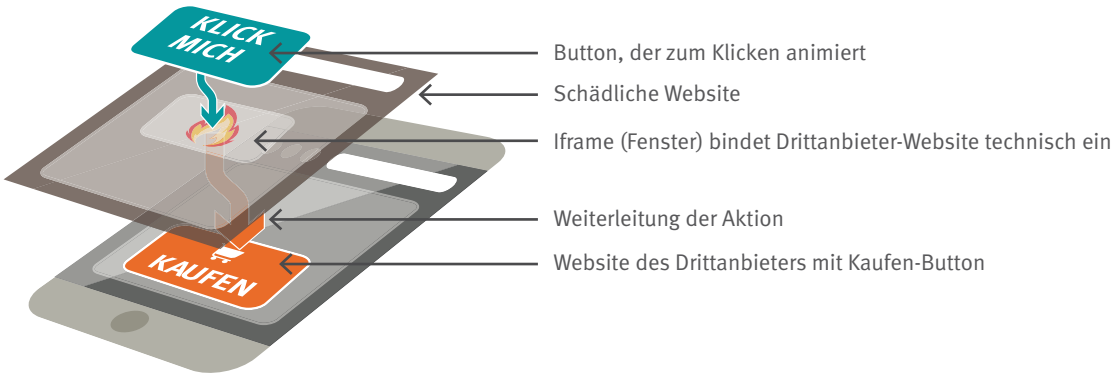
32 Den einzelnen Netzbetreibern sind verschiedene IP-Adressräume fest zugeordnet. Diese werden auch zum Aufruf der jeweiligen Redirect-Seite verwendet.

33 Siehe ausführlich in Kapitel 4.1 oder im Glossar.

34 Die MNO arbeiten derzeit an Lösungen, die eine Weitergabe der MSISDN im Rahmen einer Internet-Session nicht mehr ermöglicht.

35 Siehe Stellungnahme der Clean Market Initiative, 25.11.2016.

4 SCHEMA ZUM ANGRIFFSVEKTOR CLICKJACKING



5 VERSAND EINER SMS-BESTÄTIGUNG NACH KAUF EINER DRITTANBIETER-LEISTUNG

	Einzelkauf	Abo
Telefonica	Keine Bestäti-gungs-SMS	SMS-Versand durch Netzbe-treiber und ggf. Aggregator
Vodafone	Versand der Bestätigungs-SMS mit dem Absender „Zahl mobil“	
Telekom Deutschland	Keine Bestäti-gungs-SMS	SMS-Versand durch Aggregator oder Drittanbieter
mobilcom-debitel	In Abhängigkeit von Netzbetreiber	SMS-Versand durch Mobil-funkanbieter/ -provider oder Aggregator

a Stellungnahme der Clean Market Initiative, 25.11.2016.

Anschließend erhält der Kunde über seine Mobilfunknummer eine einmalige TAN, die er wiederum in einem zweiten Formular einträgt. Erst dann kann auch eine Berechnung über die Mobilfunkrechnung erfolgen. Unter dem Namen Web Billing (Web/TAN Flow) wird dieses Verfahren ebenfalls für den Abschluss von Abonnements über mobile Internetsessions eingesetzt.

2.3 ANGRIFFSTECHNIK UND VERBREITUNG

„Die für derartige Dienste seitens der Mobilfunknetzbetreiber zwingend vorgeschriebene Payment-Maske wird seitens des Diensteanbieters durch eine andere Seite überlagert, in der Regel durch einen PLAY-Button. Die Betätigung dieses PLAY-Buttons löst ohne Hinweis auf etwaige Kosten und ohne Kenntnis des Nutzers unmittelbar ein Abonnement aus.“[36]

Mit dieser Nachricht warnte der Deutsche Verband für Telekommunikation und Medien (DVTM)[37] im Frühjahr 2016 vor Klickbetrug (Click Fraud) im Carrier Payment-Segment.

Auch die Bundesnetzagentur konnte entsprechend unseriöse Geschäftspraktiken dokumentieren. So antwortete sie auf eine kleine Bundestagsanfrage, „dass [in den nachgewiesenen Fällen] alleine der Aufruf einer Internetseite im mobilen Internet ausreichte, um eine entsprechende Abrechnung auszulösen.“[38]

Noch einen Schritt weiter gehen die Fallbeschreibungen aus dem FWN der Verbraucherzentralen. Hier berichten Verbraucher von einem überraschenden Verhalten ihres Browsers während der mobilen Internetsitzung. So werden in manchen Fällen gleich mehrere Internetad-

36 Deutscher Verband für Telekommunikation und Medien (2016).
37 Im DVTM sind unter anderem auch Aggregatoren wie DIMOCO, first:telecom und Buongiorno Deutschland organisiert.
38 Deutscher Bundestag (2017), S. 4.

ressen nacheinander und ohne Zutun des Verbrauchers geöffnet. In anderen Fällen führt der bloße Klick auf einen Werbebanner zu einer Bestätigungs-SMS über den Abschluss eines Drittanbietervertrages.[39] Der zuletzt beschriebene Sachverhalt, auch Clickjacking[40] genannt, wurde erstmals 2008 während einer OWASP-Konferenz[41] vorgestellt.[42] Zwar wurden seitdem immer wieder unterschiedliche Arten dieses Missbrauchs bekannt[43]; es wurden aber auch immer wieder Hinweise gegeben, wie mit Clickjacking umgegangen werden kann.[44]

Ein derartiger Betrugsfall über den Browser während einer mobilen Internetsitzung ist demnach schematisch wie in Abbildung 4 dargestellt denkbar. Das Klicken auf die überlagerte Fläche kann dabei eine beliebige Reaktion zur Folge haben. In diesem Beispiel kommt es zu einer Aktivierung des Bezahlbuttons und damit zum Abschluss eines Abonnements.

Missbrauchspotenzial durch Affiliates?

Hinsichtlich potenziellen Missbrauchs verweisen die Mobilfunknetzbetreiber auf sogenannte Affiliates[45]. Diese schalten gegen Entgelt Werbung auf ihren eigenen Webseiten, über die sie Nutzer unter anderem auf Angebote von Dritten weiterleiten. Kontakt zu den Drittanbietern erhält der Affiliate über sogenannte Affiliate-Netzwerke, die entsprechende Kampagnen organisieren, das technische Instrumentarium bereitstellen und schließlich die finanzielle Ausschüttung übernehmen.

Die Verteilung der Besucherströme auf die Zielseiten erfolgt mittels verschiedenster Techniken, die auf der Webseite des Affiliates eingebaut werden müssen und zu denen beispielsweise folgende Varianten zählen:

- Das Marketingwerkzeug „URL-Generator“ wird beispielsweise mit dem Vorteil beschrieben, verschiedene Zielseiten für eine optimale Kundengewinnung anzubieten. Darüber hinaus besteht mit dieser Funktion auch die Möglichkeit, die Weiterleitung auf diverse mobile Webseiten nach dem Zufallsprinzip einzustellen.[46]
- Der Webseitenbetreiber kann außerdem ein iframe-Banner nutzen, das entsprechend den Kundenwünschen personalisiert wird, allerdings „den Vorgaben der Länder und der dortigen Betreiber entsprechen“ muss.[47]
- Letzten Endes lassen sich selbst Besucher, die sich nicht für das Angebot interessieren, beispielsweise über die Zurücktaste des verwendeten Browsers auf weitere Zielseiten leiten, wie wiederum die Methode „BackBrowser“ offeriert.[48]

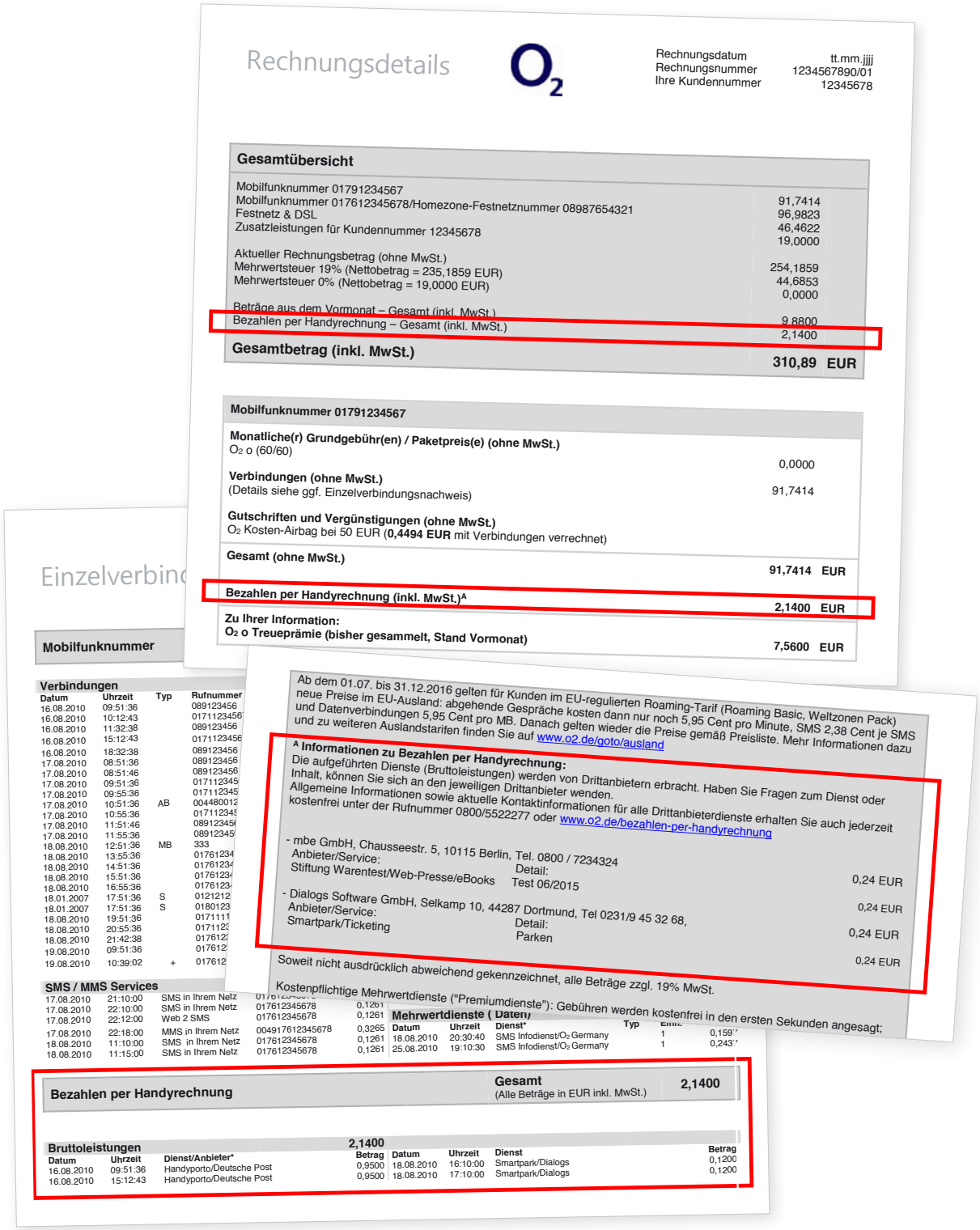
2.4 DARSTELLUNG AUF DER TELEFONRECHNUNG

Die Darstellung der abgerechneten Drittanbieterleistungen erfolgt je nach Mobilfunkanbieter in leicht abgewandelter Form. Wo sich im Gesamtrechnungsbetrag Leistungen Dritter befinden, lässt sich beispielhaft an einer O2-Rechnung[49] darstellen:

Die Posten sind sowohl als Gesamtbetrag in der „Gesamtübersicht“ der Mobilfunkrechnung abgebildet, als auch differenziert mit Datum, Uhrzeit und Betrag im Einzelverbindungsnachweis aufgeschlüsselt. Zudem finden sich weiterführende Informationen zu den Drittanbietern, beispielsweise deren Kontaktdaten, im Bereich „Gut zu wissen“ sowie am Ende der Rechnung (in Abbildung 6 nicht dargestellt).

39 Siehe Kapitel 3.1
40 Siehe dazu auch OWASP (2017).
41 OWASP: Open Web Application Security Project.
42 Vgl. Hansen und Grossmann (2008).
43 Vgl. dazu Bachfeld (2010), Schmidt (2009) oder Czumak (2013).
44 Siehe OWASP (2016).
45 Siehe auch Kapitel 4.
46 Siehe Affil4you.com (2017a).
47 Siehe Affil4you.com (2017b).
48 Siehe Affil4you.com (2017c).
49 Vgl. O2 Online (2017).

6 MUSTERRECHNUNG O2 – RECHNUNGSDETAILS



Rechnungsdetails

Rechnungsdatum tt.mm.jjjj
Rechnungsnummer 1234567890/01
Ihre Kundennummer 12345678

Gesamtübersicht

Mobilfunknummer 01791234567	
Mobilfunknummer 017612345678/Homezone-Festnetznummer 08987654321	91,7414
Festnetz & DSL	96,9823
Zusatzleistungen für Kundennummer 12345678	46,4622
	19,0000
Aktueller Rechnungsbetrag (ohne MwSt.)	254,1859
Mehrwertsteuer 19% (Nettobetrag = 235,1859 EUR)	44,6853
Mehrwertsteuer 0% (Nettobetrag = 19,0000 EUR)	0,0000
Beträge aus dem Vormonat – Gesamt (inkl. MwSt.)	9,8800
Bezahlen per Handyrechnung – Gesamt (inkl. MwSt.)	2,1400
Gesamtbetrag (inkl. MwSt.)	**310,89 EUR**

Mobilfunknummer 01791234567

Monatliche(r) Grundgebühr(en) / Paketpreis(e) (ohne MwSt.)	
O2 o (60/60)	0,0000
Verbindungen (ohne MwSt.)	
(Details siehe ggf. Einzelverbindungsnachweis)	91,7414
Gutschriften und Vergünstigungen (ohne MwSt.)	
O2 Kosten-Airbag bei 50 EUR (**0,4494 EUR** mit Verbindungen verrechnet)	
Gesamt (ohne MwSt.)	**91,7414 EUR**
Bezahlen per Handyrechnung (inkl. MwSt.)[A]	**2,1400 EUR**
Zu Ihrer Information:	
O2 o Treueprämie (bisher gesammelt, Stand Vormonat)	**7,5600 EUR**

Einzelverbin

Mobilfunknummer

Verbindungen

Datum	Uhrzeit	Typ	Rufnummer
16.08.2010	09:51:36		089123456
16.08.2010	10:12:43		0171123456
16.08.2010	11:32:38		089123456
16.08.2010	15:12:43		0171123456
16.08.2010	18:32:38		089123456
17.08.2010	08:51:36		089123456
17.08.2010	08:51:46		089123456
17.08.2010	09:51:36		017112345
17.08.2010	09:55:36		017112345
17.08.2010	10:51:36	AB	004480012
17.08.2010	10:55:36		017112345
17.08.2010	11:51:46		089123456
17.08.2010	11:55:36		089123456
18.08.2010	12:51:36	MB	333
18.08.2010	13:55:36		0176123
18.08.2010	14:51:36		0176123
18.08.2010	15:51:36		0176123
18.08.2010	16:55:36		0176123
18.01.2007	17:51:36	S	0121212
18.01.2007	17:51:36	S	0180123
18.08.2010	19:51:36		0171111
18.08.2010	20:55:36		0171123
18.08.2010	21:42:38		0176123
19.08.2010	09:51:36		0176123
19.08.2010	10:39:02	+	017612

SMS / MMS Services

17.08.2010	21:10:00	SMS in Ihrem Netz	017612345678	0,1261
17.08.2010	22:10:00	SMS in Ihrem Netz	017612345678	0,1261
17.08.2010	22:12:00	Web 2 SMS	017612345678	
17.08.2010	22:18:00	MMS in Ihrem Netz	004917612345678	0,3265
18.08.2010	11:10:00	SMS in Ihrem Netz	017612345678	0,1261
18.08.2010	11:15:00	SMS in Ihrem Netz	017612345678	0,1261

Ab dem 01.07. bis 31.12.2016 gelten für Kunden im EU-regulierten Roaming-Tarif (Roaming Basic, Weltzonen Pack) neue Preise im EU-Ausland: abgehende Gespräche kosten dann nur noch 5,95 Cent pro Minute, SMS 2,38 Cent je SMS und Datenverbindungen 5,95 Cent pro MB. Danach gelten wieder die Preise gemäß Preisliste. Mehr Informationen dazu und zu weiteren Auslandstarifen finden Sie auf www.o2.de/goto/ausland

[A] Informationen zu Bezahlen per Handyrechnung:
Die aufgeführten Dienste (Bruttoleistungen) werden von Drittanbietern erbracht. Haben Sie Fragen zum Dienst oder Inhalt, können Sie sich an den jeweiligen Drittanbieter wenden.
Allgemeine Informationen sowie aktuelle Kontaktinformationen für alle Drittanbieterdienste erhalten Sie auch jederzeit kostenfrei unter der Rufnummer 0800/5522277 oder www.o2.de/bezahlen-per-handyrechnung

- mbe GmbH, Chausseestr. 5, 10115 Berlin, Tel. 0800 / 7234324
  Anbieter/Service: Detail: 0,24 EUR
  Stiftung Warentest/Web-Presse/eBooks Test 06/2015
- Dialogs Software GmbH, Selkamp 10, 44287 Dortmund, Tel 0231/9 45 32 68,
  Anbieter/Service: Detail: 0,24 EUR
  Smartpark/Ticketing Parken 0,24 EUR

Soweit nicht ausdrücklich abweichend gekennzeichnet, alle Beträge zzgl. 19% MwSt.

Kostenpflichtige Mehrwertdienste ("Premiumdienste"): Gebühren werden kostenfrei in den ersten Sekunden angesagt;

Mehrwertdienste (Daten)

Datum	Uhrzeit	Dienst*	Typ	Einh.	
18.08.2010	20:30:40	SMS Infodienst/O2 Germany	1	0,159	
25.08.2010	19:10:30	SMS Infodienst/O2 Germany	1	0,243	

Bezahlen per Handyrechnung — **Gesamt** (Alle Beträge in EUR inkl. MwSt.) **2,1400**

Bruttoleistungen **2,1400**

Datum	Uhrzeit	Dienst/Anbieter*	Betrag
16.08.2010	09:51:36	Handyporto/Deutsche Post	0,9500
16.08.2010	15:12:43	Handyporto/Deutsche Post	0,9500
18.08.2010	16:10:00	Smartpark/Dialogs	0,1200
18.08.2010	17:10:00	Smartpark/Dialogs	0,1200

Quelle: O2 Online (2017).

3. DRITTANBIETERPROBLEMATIK AUS VERBRAUCHERSICHT

3.1 FRÜHWARNNETZWERK

Immer wieder suchen Mobilfunkkunden mit Drittanbieterproblemen die Beratungsstellen der Verbraucherzentralen auf. Im Zuge dieser Beratungen werden auffällige Sachverhalte detailliert in das FWN eingetragen, die eine Kategorisierung sowie eine anschließende qualitative Analyse ermöglicht. Diese Informationen helfen den Marktwächtern, den Markt aus der Verbraucherperspektive zu beobachten und zu untersuchen. Eine Quantifizierung der Daten aus dem FWN heraus bzw. ein Rückschluss auf die Häufigkeit des Vorkommens in der Verbraucherberatung insgesamt ist jedoch nicht möglich.

Um die im FWN vorliegenden Drittanbieterfälle differenziert auszuwerten, wurden die Fälle in unterschiedliche Kategorien (im Text gefettet dargestellt) eingeordnet. Ein besonderer Fokus wird dabei auf folgende Aspekte gelegt:

- Auslöser der Drittanbieterleistung
- Zeitpunkt der Kenntnisnahme des Verbrauchers
- Reaktionen des Verbrauchers
- Reaktionen der Unternehmen
- Kosten

Der Schwerpunkt der Untersuchung betrachtete den Zeitraum in 2016 (Kapitel 3.1.1 bis 3.1.5). Die Analyse wurde anschließend um den Betrachtungszeitraum Anfang 2017 erweitert, um Veränderungen inhaltlicher Art zu dokumentieren (Kapitel 3.1.6).

METHODIK ZUR AUSWERTUNG DES FRÜHWARNNETZWERKS

Das FWN wird anhand eines induktiv entwickelten Kategoriensystems ausgewertet. Das Ziel ist eine Clusterung der Sachverhalte und eine darauf aufbauende Auswertung der Verbraucherprobleme.[50]

Untersuchungszeiträume
01.04 – 30.06.2016 sowie 01.01.2017 – 28.02.2017

Auswertungsgrundlage
Qualitative Eingabe von Sachverhalten mittels einer browserbasierten Software durch die Beratungskräfte in den jeweiligen Verbraucherzentralen (FWN).

Auswertungsmethodik
Qualitative Inhaltsanalyse nach Mayring[51]

Vorgehensweise
Induktive Kategorienentwicklung[52]

Datengrundlage
Sachverhalte, die dem Bereich Telekommunikation innerhalb des FWN zugeordnet worden. 226 Sachverhalte Drittanbieter im Untersuchungszeitraum 2016 im Bereich Mobilfunk (255 insgesamt; 29 Festnetz oder nicht zuordenbar). 75 Sachverhalte Drittanbieter im Untersuchungszeitraum 2017.

Gütekriterien
Codierleitfaden zur Nachvollziehbarkeit des Vorgehens; Berechnung von Maßzahlen (Reliabilität nach Holsti, Krippendorfs Alpha) jeweils für Inter- und Intracoderreliabilität[53,54]

50 Vgl. Häder (2015), S. 331.
51 Vgl. Fenzl und Mayring (2014).
52 Vgl. ebda., S. 82 ff.
53 Vgl. Verbraucherzentrale Bundesverband (2016b).
54 Vgl. Mayring (2014), S. 109 ff.

3.1.1 Auslöser der Drittanbieterleistung

Abhängig von der Art des Drittanbieters können die Auslöser des Vertragsabschlusses stark variieren. Deutlich wird dies vor allem bei **absichtlichen Abschlüssen** von Drittanbieterverträgen. Manche Verbraucher rufen kostenpflichtige Rufnummern aufgrund von Fernsehwerbung oder Fernsehsendungen an; in anderen Fällen schließt das Kind der eigentlichen Vertragsperson einen Vertrag ab.

Bei der Kategorie des **unbewussten Vertragsabschlusses ohne aktive Handlung des Verbrauchers** ist hingegen völlig unklar, wie der Rechnungsposten des Drittanbieters auf die Rechnung gekommen ist. In einigen Fällen waren die Verbraucher nach eigener Aussage zum angegebenen Zeitpunkt nicht einmal in der Nähe ihres Telefons.

Anders sieht es dagegen beim **unabsichtlichen Vertragsabschluss mit aktiver Handlung des Verbrauchers** aus. So werden bei manchen Sonderrufnummern unter falschen Vorgaben Tastenbestätigungen verlangt, deren Ausführung einen hohen Preis nach sich ziehen. Beispielhaft hierfür sind sogenannte Hosentaschenanrufe, bei welchen das Mobiltelefon des Verbrauchers durch unbewussten Kontakt mit den Wahltasten eine unbestimmte Nummer anruft (56565 u. a.). In anderen Fällen wird ein Werbebanner an- oder weggeklickt, es wird eine Seite direkt oder durch eine Verlinkung aufgerufen, oder es werden nicht eindeutig gekennzeichnete Bestellbuttons angeklickt.

Insgesamt wird während der Untersuchung der Sachverhalte deutlich, dass Verbraucher auch Drittanbieterleistungen auf ihrer Rechnung bemerken, die sie nach eigener Einschätzung nicht bewusst abgeschlossen haben.

BEISPIELFALL AUS DEM FWN

„Beim mobilen surfen „poppte“ beim Verbraucher eine nicht aufgerufene Seite auf, die kostenpflichtige Leistungen im Mobilfunk anbot. Beim Versuch, diese „wegzuklicken“, kam der Verbraucher scheinbar nicht genau auf das entsprechende Kreuzchen [...]. Der Verbraucher brach diesen Vorgang direkt ab. Anschließend erhielt er eine SMS-Benachrichtigung, dass ab sofort wöchentlich 4,99 Euro berechnet werden.“

3.1.2 Kenntnisnahme des Verbrauchers

Unabhängig davon, ob ein Vertragsschluss absichtlich oder unabsichtlich ausgelöst wurde, stellt sich die Frage, wann der Verbraucher vom Abschluss der Drittanbieterleistung erfahren hat. Dies kann **unmittelbar** erfolgen, da der Verbraucher ohne große Zeitverzögerung durch eine Bestätigungs-SMS informiert wird. Der Inhalt einer solchen SMS ist unterschiedlich und enthält mitunter Angaben zum Preis, Anbieter, Produkt sowie Kontaktinformationen.

Teilweise erfährt der Verbraucher allerdings erst **später**, dass ein Entgelt in Rechnung gestellt wurde. So entdeckt er beispielsweise die Kosten für ein Abonnement oder einen Einzelabruf erst beim Lesen der monatlichen Mobilfunkrechnung oder bei einer rein summarischen Prüfung der Rechnung.

Das folgende Beispiel zeigt eine Informations-SMS zum Drittanbietervertrag:

BEISPIELFALL AUS DEM FWN

„Sehr geehrter Kunde, der Dienst [XXX] hat soeben über Ihre Handyrechnung 4,99 Euro abgerechnet. Kontaktinformationen, 0800 XXXXXXX, info@xxxxxxx.xx erreichbar werktags 08–22 Uhr, sonst 09–18 Uhr. Mehr Informationen zur Abo-Verwaltung erhalten Sie unter http:// xxxxxxx.xx“

3.1.3 Reaktionen der Verbraucher

Die Reaktionen der Verbraucher wurden in zwei Unterkategorien geordnet:

- Allgemeine Reaktionen
- Reaktionen der Verbraucher gegenüber den Unternehmen

Bei den **allgemeinen Reaktionen** konnten unterschiedliche Verhaltensweisen beobachtet werden. Während viele Verbraucher die **Konsequenzen**, beispielsweise einer Bestätigungs-SMS (siehe nachfolgendes Beispiel), **falsch einschätzen**, begeben sich andere wiederum auf

die eigenständige **Recherche** zur Drittanbieterthematik. In weiteren Fällen wenden sich Betroffene mit ihren **Anfragen an andere Institutionen**, wie der Polizei oder der Bundesnetzagentur.

BEISPIELFALL AUS DEM FWN

„Der Verbraucher bekam eine SMS mit den Worten „Herzlichen Glückwunsch zu ihrem abgeschlossenen Abo für 7,99 Euro die Woche". Er dachte an einen Virus und löschte diese direkt […]."

Auch in den **Reaktionen gegenüber den Unternehmen** lassen sich unterschiedliche und kombinierbare Handlungsweisen erkennen. Der Verbraucher:

- **kündigt** das Abo,
- **bezahlt** die geforderten Abo-Kosten,
- **lehnt** die Zahlung grundsätzlich **ab**,
- lässt strittige Beträge von seiner Bank zurückbuchen,
- lässt sich eine Drittanbietersperre einrichten,
- fordert die Herausgabe der Adressen der Drittanbieter,
- verlangt einen Nachweis über den Vertragsabschluss,
- stellt **allgemeine Anfragen**, wenn er den Sachverhalt noch nicht genau kennt.

Letzteres tritt insbesondere in den Fällen auf, in denen Verbraucher aufgrund ihrer Unsicherheit in dieser spezifischen Situation noch **keinen Kontakt zu ihrem Vertragspartner** aufgenommen haben und sich zuerst bei anderen Institutionen erkundigen.

BEISPIELFALL AUS DEM FWN

„Die Kundin bemerkte […] sieben Drittanbieterbelastungen, die ihr völlig unerklärlich sind. Sie hat Einspruch gegen die Rechnung erhoben und, soweit noch nicht vorhanden, auch die zustellfähigen Anschriften der Drittanbieter angefordert […]"

Die Vielzahl der dargestellten Reaktionen zeigt, dass es Verbraucher gibt, die offensiv gegenüber den beteiligten Unternehmen reagieren, indem sie strittige Beträge zurückbuchen oder eine Drittanbietersperre fordern etc. Aber, wie die Erfahrungen aus den Verbraucherzentralen zeigen, gibt es gleichzeitig auch zahlreiche Verbraucher, die zusätzliche Informationen und weitergehende Unterstützung benötigen. Dies äußert sich unter anderem in der Inanspruchnahme alternativer Ansprechpartner, wie zum Beispiel der Verbraucherzentrale.

In den meisten Fällen ist allerdings der **Telekommunikationsanbieter** der für den Verbraucher wichtigste Ansprechpartner, darüber hinaus werden auch die **Aggregatoren** sowie die **Drittanbieter** selbst von Verbrauchern angesprochen. In seltenen Fällen, wenn der Streit um die Bezahlung eskaliert, treten **Inkassounternehmen** als vorrangige Ansprechpartner auf.

3.1.4 Reaktionen der jeweilig angesprochenen Unternehmen

Als **kooperativ** werden die Unternehmen kategorisiert, die auf Anfragen der Verbraucher mit einer konstruktiven Hilfestellung reagieren – unabhängig von dem rechtlichen Hintergrund dieser Verhaltensweise. Beispielhaft kann man hier folgende Reaktionen nennen:

- Die Einrichtung einer Drittanbietersperre,
- Eine vollumfängliche oder partielle Rückerstattungen der Drittanbieterbeträge,
- Die Kündigung des Abos wird meistens von den Aggregatoren, teilweise aber auch von den Telekommunikationsunternehmen vorgenommen

BEISPIELFALL AUS DEM FWN

„Der Vertragspartner hat dem Kunden die ladungsfähige Anschrift mitgeteilt und 140 Euro gutgeschrieben."

Allerdings konnten auch Fälle mit **unkooperativen** Reaktionen der Unternehmen beobachtet werden. Dazu zählen die folgenden Vorgehensweisen:

- Betroffene Verbraucher werden zur Klärung des Sachverhalts **an den jeweiligen Drittanbieter verwiesen**.
- Weigert sich der Verbraucher, den geforderten Betrag zu bezahlen oder bucht die Lastschriften zurück, **droht der Anbieter** in einigen Fällen **mit einer Sperre des Anschlusses und/oder führt diese auch durch**. Diese Sperre wird nur angedroht, wenn die Unternehmen den Standpunkt ihrer Forderung aufrechterhalten.
- Die beteiligten Unternehmen **leisten keine Hilfestellung** und weisen die Verantwortung für die Abrechnung von sich.

In anderen Sachverhalten sind zudem auch **weitergehende Maßnahmen** zu beobachten. So kommt es zu Mahnungen, und in einigen Fällen drohen Telekommunikationsanbieter auch mit der Kündigung des Anschlusses und der Einschaltung eines Inkasso-Unternehmens.

BEISPIELFALL AUS DEM FWN

„Die Verbraucherin versuchte bereits eine Drittanbietersperre einrichten zu lassen (für die Zukunft), aber sowohl der Vertragspartner – als auch die Mitarbeiter des Netzbetreibers in den Shops behaupteten, dass das für Prepaidverträge nicht möglich sei und sie dafür auch gar nicht zuständig seien. […]“

Wird das Unternehmen nach einem Nachweis über das Zustandekommen des Vertrages gebeten, dann berichten Verbraucher auch hier von unterschiedlichen Reaktionen. Wird ein **Nachweis vorgelegt**, dann beinhaltet dieser meist ein technisches Prüfprotokoll oder einen Einzelverbindungsnachweis. In einigen Fällen ist es allerdings so, dass der Anbieter **keine** oder **nur unvollständige Nachweise** vorlegt. Im letzteren Fall wird argumentiert, dass der Vertragsschluss durch Tastendruck am Telefon oder durch einen Klick auf einen Banner belegt sei.

BEISPIELFALL AUS DEM FWN

„Der Verbraucher hat fristgerecht (insgesamt 2 Mal) das technische Prüfprotokoll angefordert. Der Vertragspartner hat nicht reagiert.“

Die Kategorie **besondere Reaktionen der Anbieter** ist vereinzelt im FWN anzutreffen. So wird Verbrauchern, welche sich mit der Bitte um die Einrichtung einer Drittanbietersperre an ihren Telekommunikationsanbieter wenden, die Auskunft erteilt, dass dies nur gegen ein Entgelt möglich wäre. Seltener kommt es vor, dass Mitarbeiter von Telekommunikationsunternehmen den Verbraucher an die Verbraucherzentralen weiterleiten.

3.1.5 Kosten für Abonnements

Die Kosten **für ein einzelnes Abo** im Abrechnungszeitraum liegen, sofern angegeben, in allen Fällen unter 10 Euro. Die Preisspanne bewegt sich hierbei von 4,99 Euro bis 9,99 Euro pro Woche; häufig wird auch 6,99 Euro pro Woche genannt. Ebenso können Abos auch monatlich abgerechnet werden. Hier kann sich die Preisspanne eines einzeln abgeschlossenen Abos im zweistelligen Bereich bewegen. Die **Gesamtkosten** der einzelnen Fälle im FWN sind ungleich verteilt. Abhängig von der Drittanbieterleistung werden einzelne Rechnungen mit Kosten von wenigen Euro bis zu mehreren Tausend Euro beziffert.

BEISPIELFÄLLE AUS DEM FWN

„Es bestehen Drittanbieterabos von 10 Firmen. […] Schaden 619,79 Euro.“
„Dem Verbraucher wurden Kosten von insgesamt 6385,00 Euro für sogenannte Premium-SMS in Rechnung gestellt.“

3.1.6 Beobachtungen aus dem Frühwarnnetzwerk 2017

Um aktuelle Entwicklungen zu beobachten, wurde das FWN mit Hinblick auf die Drittanbieterproblematik genauer untersucht. Die in den Monaten Januar 2017 und Februar 2017 in das FWN gemeldeten Drittanbieter-Sachverhalte zeigen inhaltlich ein ähnliches Bild wie in der vorhergehenden Auswertung aus dem Jahr 2016. Weiterhin schildern Verbraucher in den Beratungsstellen ihre Probleme mit Drittanbietern auf der Mobilfunkrechnung. Teilweise beziehen sich diese Beschwerden noch auf das Jahr 2016. In anderen Fällen sind die Verträge über Drittanbieterleistungen erst im Jahr 2017 zustande gekommen beziehungsweise wurden diese erst dann abgerechnet.

Nach einer Auswertung von insgesamt 75 Sachverhalten in diesem Zeitraum zeigt sich, dass in der Kategorie Auslöser des Drittanbieters der „unbewusste Vertragsabschluss“ neben der Kategorie „keine Angabe“ von Verbrauchern einen Schwerpunkt bildet. Dies verdeutlicht auch folgender Beispielsachverhalt, in welchem eine Verbraucherin über Facebook eine angebliche Produkttester-App heruntergeladen haben soll.

BEISPIELFÄLLE AUS DEM FWN

„[…] Nach dem Herunterladen der App erhielt die Verbraucherin 3 SMS mit Codes, die sie im Internet eingeben sollte, um die Bezahlung auszulösen. Die Codes hat die Verbraucherin nicht eingegeben. Dennoch wurde ihre Mobilfunkrechnung mit 3 mal 59,00 Euro durch die [xxx] belastet.[…] Es besteht die Befürchtung, dass die App die SMS ausgelesen haben könnte und so ein Eintrag möglich war.“

„Am 14.01.2017 erschien bei der Verbraucherin auf dem Handy ein großer weißer Pfeil, der nicht mehr weg ging. Verbraucherin schloß daraufhin die offenen Seiten und erhielt zwei SMS mit der Mitteilung, dass ein Abo abgeschlossen wurde. Keine Redirect-Lösung des Netzbetreibers zu beobachten.“

In vielen Fällen nehmen Verbraucher erst beim Einsehen in die Rechnung Kenntnis von der Abbuchung und dem vermeintlichen Vertragsschluss. Auch in Bezug auf die Reaktionen der Verbraucher sowie der Mobilfunkanbieter sind keine wesentlichen Veränderungen zu beobachten. Demnach lässt sich festhalten, dass die Problematik in Bezug auf strittige Drittanbieterleistungen auf der Mobilfunkrechnung, die beispielsweise über eine mobile Internetverbindung oder eine Kurzwahlnummer zustande kamen, auch weiterhin besteht.

3.2 AUSPRÄGUNGEN IN DER BEVÖLKERUNG – REPRÄSENTATIVE UMFRAGE

Um Aussagen über die Relevanz der möglichen Drittanbieterproblematik in der Bevölkerung treffen zu können, sowie weitere Aspekte zu dieser Thematik zu beleuchten, wurde eine bevölkerungsrepräsentative Umfrage durchgeführt. Dazu wurde aufbauend auf der FWN-Analyse ein Fragebogenentwurf entwickelt und mit den bundesweiten Telekommunikationsexperten der Verbraucherzentralen abgestimmt. Die erkenntnisleitenden Fragen sind den folgenden Passagen vorangestellt.

Welche Relevanz hat das Bezahlen von Drittanbieterleistungen über die Mobilfunkrechnung unter Mobilfunknutzern in der Bevölkerung?

Im Rahmen der Umfrage hat sich ergeben, dass die Funktion „Bezahlen über die Mobilfunkrechnung“ mehrheitlich (89 Prozent) von den befragten Mobilfunknutzern nicht genutzt wird. Bei lediglich acht Prozent der Mobilfunknutzer tauchten innerhalb der letzten drei Jahre vor dem Befragungszeitpunkt Rechnungsbeträge für Drittanbieterleistungen auf der Mobilfunkrechnung auf bzw. wurden vom Guthaben abgebucht.

Dabei ist zu beachten, dass das Auftauchen von Rechnungsbeträgen auf der Telefonrechnung noch offen lässt, ob der Abschluss der Drittanbieterleistungen absichtlich oder unabsichtlich erfolgte (siehe Abbildung 7).

Wie hoch ist der Anteil von Mobilfunknutzern, die Drittanbieterleistungen unabsichtlich abgeschlossen haben?

Von den Mobilfunknutzern, die innerhalb der letzten drei Jahre abgeschlossene Drittanbieterleistungen auf ihrer Mobilfunkrechnung hatten bzw. denen Beträge vom

Prepaidguthaben abgebucht wurden, geben 61 Prozent bei der geschlossenen Frage[55] an, dass sie diese immer unabsichtlich abgeschlossen haben. Für 33 Prozent der Befragten dieser Untergruppe erfolgte der Abschluss immer absichtlich (siehe Abbildung 8).

Laut Untersuchungsergebnissen haben demnach lediglich ein Drittel der Befragten (gestützte Abfrage) Drittanbieterleistungen ausschließlich absichtlich abgeschlossen. Bezogen auf die Grundgesamtheit der Mobilfunknutzer bedeutet dies, dass rund fünf Prozent der Mobilfunknutzer in den vergangen drei Jahren schon einmal unabsichtlich Drittanbieterleistungen abgeschlossen haben. Bei lediglich drei Prozent der Mobilfunknutzer erfolgte der Abschluss „immer absichtlich“ (vgl. Abbildung 9).

Unter Berücksichtigung der statistischen Fehlertoleranz lässt sich hochrechnen, dass schätzungsweise **2,2 bis 3,4 Millionen** der deutschsprachigen Mobilfunknutzer ab 14 Jahren in Deutschland, in den vergangenen 3 Jahren vom unabsichtlich Abschluss von Drittanbieterleistungen betroffen waren.[56]

Insbesondere Nutzer von Prepaidverträgen haben oftmals Probleme, den unabsichtlichen Abschluss eines Drittanbietervertrages zu bemerken, da sie keinen rechtlichen Anspruch auf eine Rechnungsübersicht haben. Die Untersuchungszahlen zeigen, dass mehr als ein Drittel der Mobilfunknutzer (38 Prozent) für ihr hauptsächlich genutztes Mobilfunkgerät einen oder mehrere Prepaid-Verträge bzw. eine Kombination aus Laufzeit- und Prepaidverträgen (zum Beispiel für ein Dual-Sim-Mobiltelefon) abgeschlossen haben.

METHODENSTECKBRIEF

Erhebungszeitraum 3. – 24. August 2016

Grundgesamtheit
In Privathaushalten in Deutschland lebende deutschsprachige Mobilfunknutzer ab 14 Jahren

Stichprobendesign
Dual-Frame-Ansatz (Festnetz- sowie Mobilfunkstichprobe)

Erhebungsmethodik
Computergestützte Telefonumfrage (Computer Assisted Telephone Interview; CATI)[a]

Auswahlgrundlage und -verfahren
ADM Telefon-Mastersample/Last-Birthday-Methode

Nettostichprobe n = 1.517 Personen

Gewichtung
Gewichtung der Ausgangsstichprobe nach Region, Geschlecht, Alter und Bildung

Statistische Fehlertoleranz
zwischen ± 1,1 Prozent-Punkte (bei Stichproben-Anteilswerten von 5 Prozent oder 95 Prozent) und ± 2,5 Prozent-Punkte (bei einem Stichproben-Anteilswert von 50 Prozent)

Durchführendes Institut
forsa.main Marktinformationssysteme GmbH

[a] https://ssl.marktwaechter.de/sites/default/files/downloads/fragebogen-marktwaechteruntersuchung.pdf

Hochgerechnet auf die deutschsprachigen Mobilfunknutzer ab 14 Jahren entspricht der Anteil von 38[57] Prozent in der Grundgesamtheit 22,3[58] Millionen Personen, für

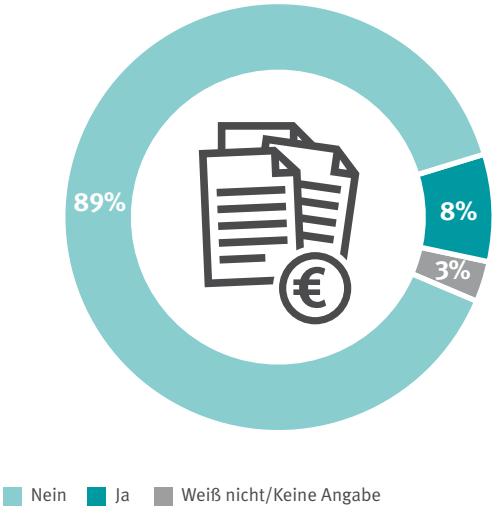
55 Damit die Untersuchungsteilnehmer bei der Beantwortung der Frage, ob der Abschluss absichtlich und/oder unabsichtlich war, nicht durch den Interviewer möglicherweise in eine Richtung gelenkt werden, erfolgte die Messung zweistufig. Dazu sollten die betroffenen Mobilfunknutzer im ersten Schritt im Rahmen einer offenen Frage schildern, wie es zum Abschluss der Drittanbieterleistung gekommen ist (ungestützte Abfrage). Im Anschluss wurde mittels einer geschlossenen Frage erhoben, ob der Abschluss der Drittanbieterleistung absichtlich und/oder unabsichtlich erfolgte (gestützte Abfrage).

56 Basis: Mobilfunknutzer, die Angaben zu ihrer Vertragsart sowie ihrem Anbieter machen konnten. Hochrechnung aus Marktwächter-Befragungsergebnissen 2016 (Basis der Stichprobe: n=1.442 deutschsprachige Mobilfunknutzer (Handy-, Smartphone und Tablet-Nutzer mit SIM-Karte) ab 14 Jahren in Privathaushalten in Deutschland mit Kenntnis ihres Mobilfunkanbieters; Basis für die Hochrechnungen: Mobilfunknutzer aus dem forsa-Mehrthemenbus sowie Bevölkerungsfortschreibung per 31.12.2014 des Statistischen Bundesamtes).

57 Schwankungsbreite ±2,44 Prozent.

58 Hochrechnung aus Marktwächter-Befragungsergebnissen 2016 (Basis der Stichprobe: n=1.442 deutschsprachige Mobilfunknutzer (Handy-, Smartphone und Tablet-Nutzer mit SIM-Karte) ab 14 Jahren in Privathaushalten in Deutschland mit Kenntnis ihres Mobilfunkanbieters; Basis für die Hochrechnungen: Mobilfunknutzer aus dem forsa-Mehrthemenbus sowie Bevölkerungsfortschreibung per 31.12.2014 des Statistischen Bundesamtes).

7 BEZAHLEN VON DRITTANBIETERLEISTUNGEN ÜBER DIE MOBILFUNKRECHNUNG



Frage 6a: Hatten Sie innerhalb der letzten drei Jahre schon einmal Rechnungsbeträge für Leistungen auf Ihrer Mobilfunkrechnung oder wurden Beträge von Ihrem Guthaben abgebucht, die nicht von Ihrem Mobilfunkanbieter waren, sondern von sogenannten Drittanbietern? Damit meinen wir zum Beispiel Kosten für Auskunftsdienste, Horoskope, Emoticons, Klingeltöne, Musik, Telefon-Voting oder Parktickets.

Frage 6b (Frageformulierung für Prepaid-Nutzer): Wurden Ihnen innerhalb der letzten drei Jahre schon einmal Rechnungsbeträge für Leistungen von Ihrem Guthaben abgebucht, […].

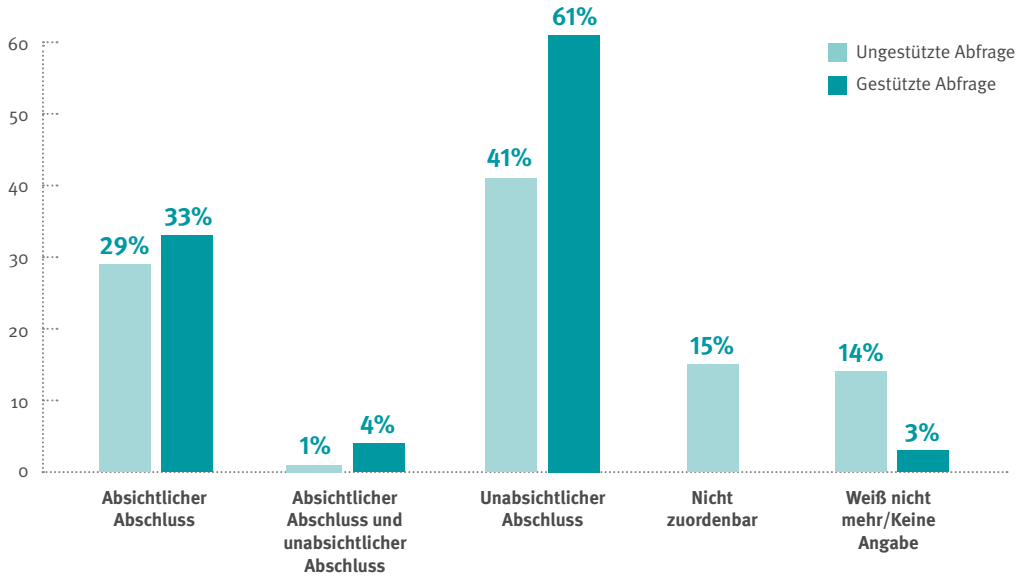
Frage 6c (Frageformulierung für Nicht-Rechnungsempfänger): Auch wenn Sie nicht persönlich der Rechnungsempfänger sind: […].

Basis: Mobilfunknutzer mit Angabe der Vertragsart und des Mobilfunkanbieters (n = 1.442).

8 VERTEILUNG ABSICHTLICHER UND UNABSICHTLICHER ABSCHLUSS VON DRITTANBIETERLEISTUNGEN

Frage 7a: Bitte schildern Sie mir einmal, wie es zum Abschluss der Leistung beim Drittanbieter kam.

Frage 7b: Und haben Sie die Leistung beim Drittanbieter immer absichtlich abgeschlossen oder immer unabsichtlich? Oder ist es auch vorgekommen, dass Sie eine Drittanbieterleistung manchmal absichtlich und manchmal unabsichtlich abgeschlossen haben?



Basis: Mobilfunknutzer, denen Drittanbieterleistungen in Rechnung gestellt wurden oder vom verfügbaren Guthaben abgebucht wurden (n = 118).

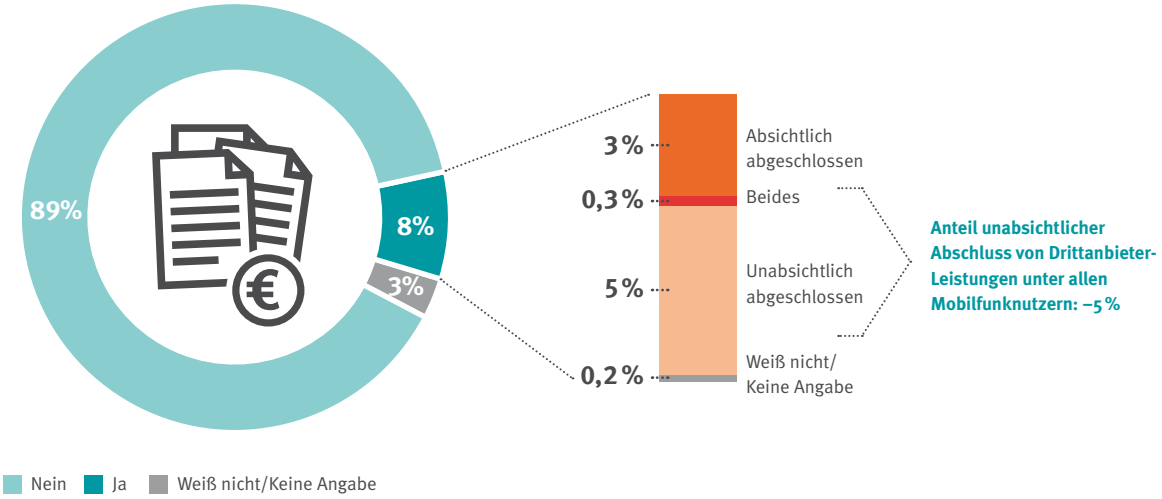
9 BEZAHLEN VON DRITTANBIETERLEISTUNGEN ÜBER DIE MOBILFUNKRECHNUNG NACH ABSCHLUSSART

Frage 6a: Hatten Sie innerhalb der letzten drei Jahre schon einmal Rechnungsbeträge für Leistungen auf Ihrer Mobilfunkrechnung oder wurden Beträge von Ihrem Guthaben abgebucht, die nicht von Ihrem Mobilfunkanbieter waren, sondern von sogenannten Drittanbietern? Damit meinen wir zum Beispiel Kosten für Auskunftsdienste, Horoskope, Emoticons, Klingeltöne, Musik, Telefon-Voting oder Parktickets.

Frage 6b: Wurden Ihnen innerhalb der letzten drei Jahre schon einmal Rechnungsbeträge für Leistungen von Ihrem Guthaben abgebucht, […].

Frage 6c: Auch wenn Sie nicht persönlich der Rechnungsempfänger sind: […].

Frage 7b: Und haben Sie die Leistung beim Drittanbieter immer absichtlich abgeschlossen oder immer unabsichtlich? Oder ist es auch vorgekommen, dass Sie eine Drittanbieterleistung manchmal absichtlich und manchmal unabsichtlich abgeschlossen haben?



Basis: Mobilfunknutzer mit Angabe der Vertragsart und des Mobilfunkanbieters (n = 1.442).

die sich die Rechnungseinsicht schwierig gestaltet bzw. nicht möglich ist.

Jedoch stellt auch der Erhalt einer Rechnung nicht immer sicher, dass unabsichtliche Abschlüsse zwangsläufig umgehend vom Mobilfunkkunden bemerkt werden. So prüfen 17 Prozent ihre Rechnung nie oder nicht persönlich, meist weil sie ihrem Anbieter vertrauen (23 Prozent) oder weil diese Aufgabe von jemand anderem aus ihrem Umfeld wahrgenommen wird (21 Prozent). Lediglich etwa die Hälfte (51 Prozent) der Mobilfunknutzer mit Laufzeitverträgen, die in der Grundgesamt 61 Prozent ausmachen (35,8 Millionen, ±2,44 Prozent), prüfen überhaupt ihre Mobilfunkrechnung „immer“ (vgl. Abbildung 11).

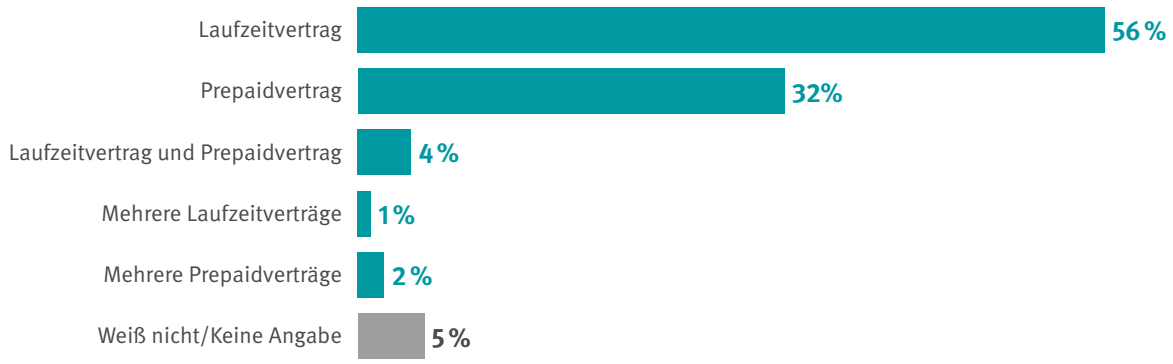
Wie hoch sind die Kosten von unabsichtlich abgeschlossenen Drittanbieterleistungen?

Die Spannbreite der Gesamtkosten durch den unabsichtlichen Abschluss von Drittanbieterleistungen innerhalb eines Jahres (inkl. möglicher Mahnkosten, Inkassogebühren, Anwaltsgebühren o. ä.) je betroffenem Verbraucher reicht von 1 Euro bis 1.000 Euro (jeweils auf volle Eurobeträge gerundet).[59] Die häufigste Nennung (Modus) in der Stichprobe ist der Betrag von 5 Euro. Bezogen auf die letzten drei Jahre vor der Untersuchung betragen

59 Allgemeine Hinweise zu den Kostenhöhen: Premium-SMS (Kosten von 29 Cent bis 6 Euro pro SMS möglich); Kurzwahldienste z. für die Auskunft (11833 kostet 1,99 Euro die Minute); Sonderrufnummern bspw. Für Tele-Voting (Festnetz 0,49 Euro pro Anruf, Mobilfunk ggf. abweichend).

10 HÄUFIGKEITSVERTEILUNG DER VERTRAGSARTEN

Frage 1: Welche Art von Vertrag haben Sie für Ihr [hauptsächlich genutztes Gerät] abgeschlossen?
Haben Sie einen Vertrag mit fester Laufzeit, bei dem Sie jeden Monat nachträglich eine Rechnung über Ihre angefallenen Mobilfunkkosten bekommen, oder haben Sie einen sogenannten Prepaid-Vertrag, bei dem Sie Ihr Guthaben für Telefonate, SMS und Internetnutzung im Voraus aufladen?



Basis: Alle befragten Mobilfunknutzer (n = 1.517).

die durchschnittlichen Kosten 86,52 Euro, wobei dieser Wert aufgrund der rechtsschiefen Verteilung (vgl. Abbildung 13) als zu hoch angesehen werden muss. Einen realistischeren Wert ergibt in diesem Fall der Median: Für 50 Prozent der befragten Mobilfunknutzer liegen die Kosten unter 25,52 Euro, während für die verbleibenden 50 Prozent die Kosten über diesem Wert liegen.

Bei 35 Prozent der Mobilfunknutzer sind durch den unabsichtlichen Abschluss von Drittanbieterleistungen Gesamtkosten bis zu 19 Euro entstanden. Bei 20 Prozent der Geschädigten liegen die Kosten bei 90 Euro oder mehr.

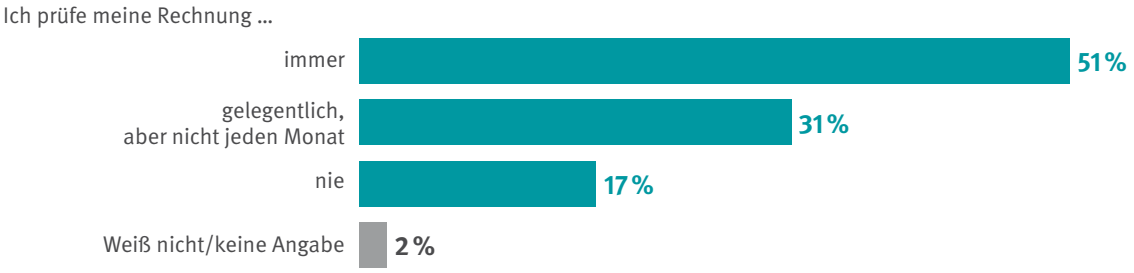
Auf Basis der ermittelten Personenanzahl von 2,2 bis 3,4 Millionen Mobilfunknutzer, die durch ein Abo geschädigt wurden, lässt sich eine Schätzung über die in den vergangenen drei Jahren entstandenen Gesamtkosten in der betroffenen Personengruppe vornehmen. Diese werden vereinfacht nach folgender Formel berechnet:

Aufgrund der Asymmetrie der Verteilung stellt das arithmetische Mittel keine geeignete Größe für die Berechnung dar (siehe oben), sodass auf den Median zurückgegriffen wird. Setzt man die bereits ermittelte Personenanzahl von **2,2 bis 3,4 Millionen** betroffenen Mobilfunknutzern in diese Formel, dann ergibt sich ein Schätzintervall für die Gesamtschadenssumme von **56.144.000 Euro bis 86.768.000 Euro**. Dabei ist zu berücksichtigen, dass die in die Berechnung eingeflossen Kosten auf volle Eurobeträge gerundet wurden und mögliche nachträgliche Erstattungen (teilweise oder ganz) nicht berücksichtigt wurden. Unter den vorgenannten Bedingungen bedeutet dies, dass den Mobilfunknutzern ab 14 Jahren in Deutschland in den 3 Jahren bis zum Untersuchungszeitpunkt (August 2016) konservativ geschätzt ein Gesamtschaden in Höhe von **56,1 bis 86,8 Millionen Euro** entstanden ist.

GESAMTSCHADENSSUMME DER MOBILFUNKNUTZER = **ANZAHL DER BETROFFENEN MOBILFUNKNUTZER** × **SCHADENSSUMME PRO MOBILFUNKNUTZER**

11 HÄUFIGKEITSVERTEILUNG DER ÜBERPRÜFUNG DER MOBILFUNKRECHNUNG

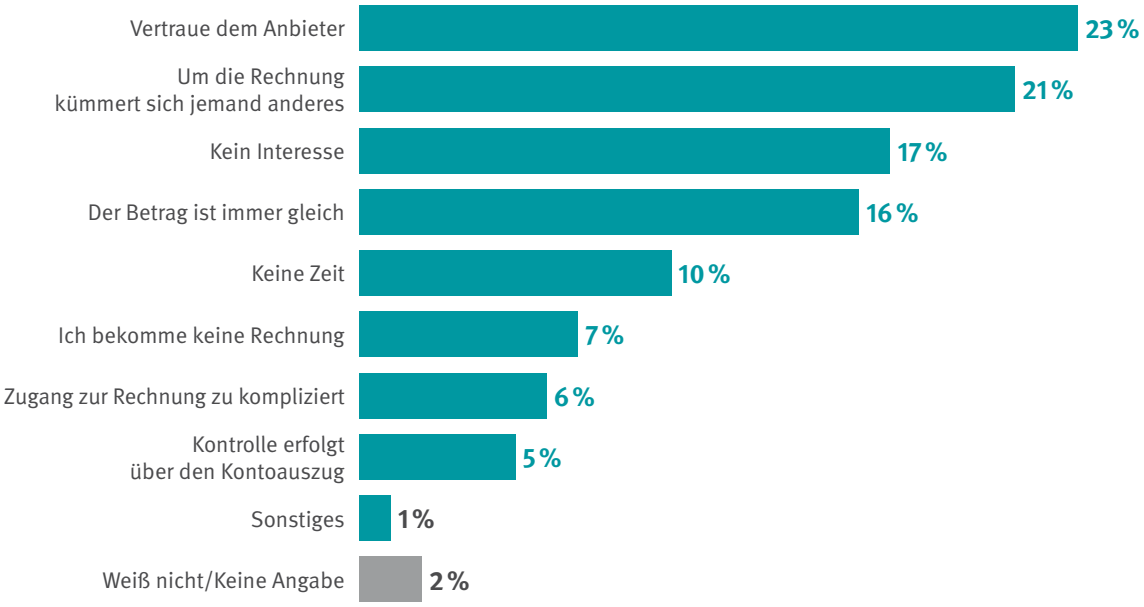
Frage 4: Wie häufig überprüfen Sie Ihre monatliche Mobilfunkrechnung? Würden Sie sagen ...



Basis: Mobilfunknutzer mit einem Laufzeitvertrag, die auch Rechnungsempfänger sind (n = 891).

12 GRÜNDE FÜR DAS NICHT-PRÜFEN DER MOBILFUNKRECHNUNG

Frage 5: Warum überprüfen Sie Ihre Mobilfunkrechnung nie? (Mehrfachantwort)



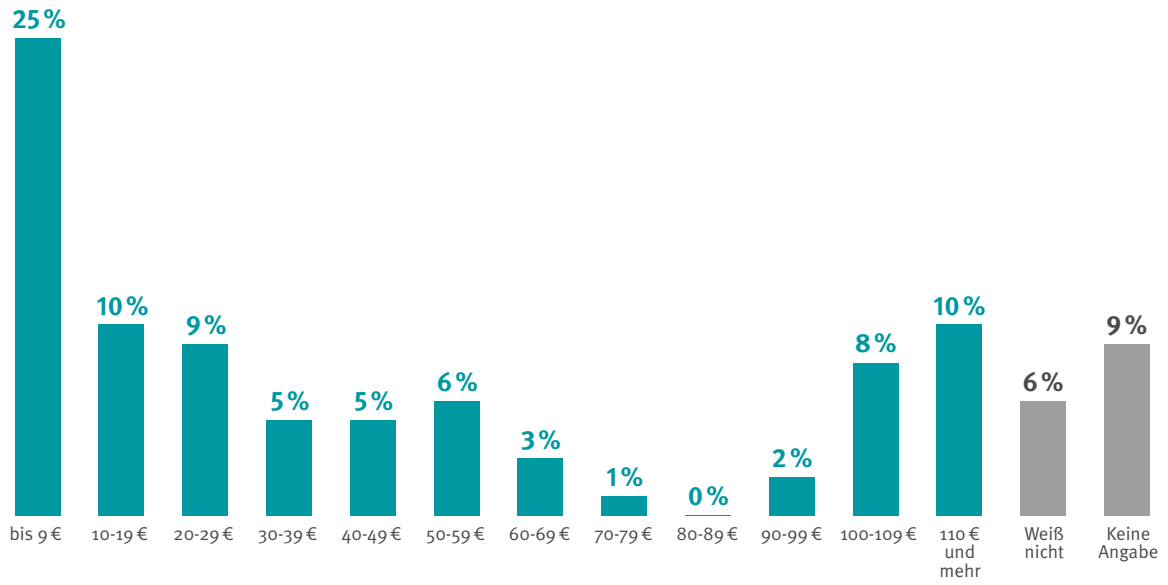
Basis: Mobilfunknutzer mit einem Laufzeitvertrag, die auch Rechnungsempfänger sind und ihre Rechnung nie prüfen (n = 148).

3.3 ZUSAMMENFASSUNG – DRITTANBIETERPROBLEMATIK AUS VERBRAUCHERSICHT

Zusammenfassend ist festzustellen, dass ein Vertrag über Drittanbieterleistungen überwiegend unabsichtlich, teilweise sogar unbewusst, abgeschlossen wird. Nicht immer erhält der Verbraucher dabei eine SMS als Bestätigung des Abschlusses, so dass diesbezügliche

13 SCHADENSSUMMEN DURCH UNABSICHTLICHEN ABSCHLUSS VON DRITTANBIETERLEISTUNGEN

Frage 8: Wie hoch waren die Gesamtkosten also inklusive möglicher Mahnkosten, Inkassogebühren, Anwaltsgebühren o. ä., die Ihnen durch den unabsichtlichen Abschluss von Drittanbieterleistungen im einem Jahr entstanden sind?



Basis: Mobilfunknutzer mit unabsichtlich abgeschlossenen Drittanbieterleistungen (n = 76).

Kosten erst später anhand der Rechnung auffallen können. Hier sind insbesondere Prepaidnutzer im Nachteil, da sie aufgrund der rechtlichen Konstellation keinen Anspruch auf eine Rechnungsübersicht haben, sodass entsprechende Leistungen schwer nachvollziehbar sind.

Wie die Erfahrungen aus der Verbraucherberatung zeigen, fragen Verbraucher bei unabsichtlichen und unbewussten Abschlüssen in den Beratungsstellen häufig zusätzliche Informationen und weitergehende Unterstützung nach. Dies ist umso verständlicher, da Mobilfunkanbieter sich nicht immer kooperativ gegenüber den Betroffenen zeigen, beispielsweise indem sie mit Mahnungen oder Sperrandrohungen weiter Druck auf die Verbraucher ausüben.

Auch wenn der Schaden strittiger Drittanbieterleistungen häufig nur im einstelligen Bereich liegt, sind ebenfalls Fälle bekannt, bei denen Verbraucher Kosten in vierstelliger Höhe in Rechnung gestellt wurden. Eine auf Basis der repräsentativen Ergebnisse erstellte Schätzung weist in der Zeit von August 2013 bis August 2016 auf eine Gesamtschadenssumme in Höhe von 56,1 bis 86,8 Millionen Euro hin.

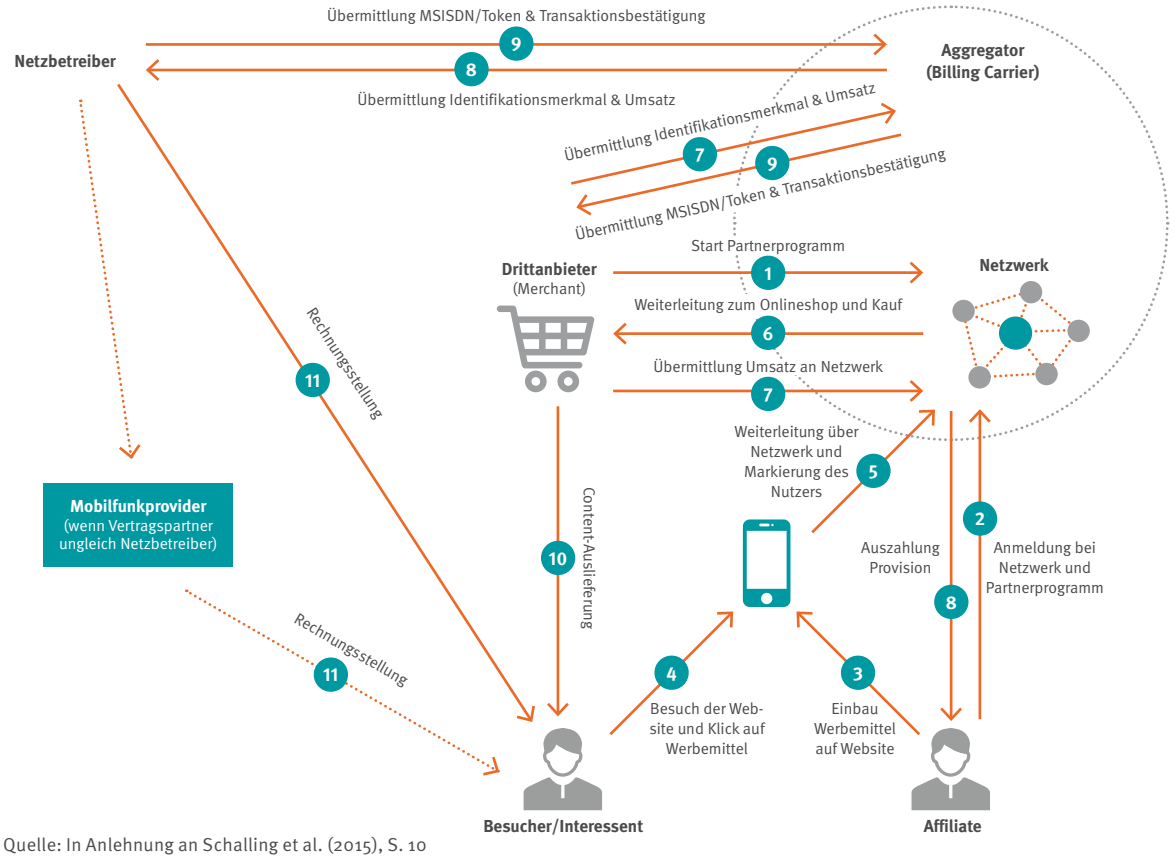
Trotz zwischenzeitlich anbieterseitig initiierter Maßnahmen sind auch im Jahr 2017 noch Fälle unbeabsichtigter Vertragsabschlüsse mit Drittanbietern in den FWN evident. Der Auslöser für die Drittanbieterleistung ist dabei nicht eindeutig. Der unbewusste Vertragsschluss wird unter anderem der hintergründigen Aktivität einer App zugeordnet, es wird in Einzelfällen auch von fehlenden Redirect-Lösungen der Netzbetreiber berichtet.

4. DRITTANBIETERMARKT UND SICHERUNGSMECHANISMEN

4.1 AKTEURE IM DRITTANBIETERMARKT

Bei dem hier betrachteten Direct Billing treten in der Regel mehrere Akteure auf, denen im Buchungsprozess eines Drittanbieter-Abonnements unterschiedliche Funktionen zukommen. Diese lassen sich anhand eines Nutzungsablaufs wie nachfolgend darstellen:

14 AKTEURE IM DRITTANBIETERMARKT



Quelle: In Anlehnung an Schalling et al. (2015), S. 10
Die Zahlen geben die Reihenfolge im Ablauf wider.

Der **Verbraucher** geht mit seinem Mobiltelefon ins Internet, wobei er direkt – durch Kenntnis der Webadresse, über eine Suchmaschine oder über sogenannte **„Affiliates“**[60] – auf das Angebot eines Drittanbieters kommt beziehungsweise dorthin geleitet wird. Von den Mobilfunknetzbetreibern (MNO)[61] werden die Affiliates darüber hinaus als potentielle Gefahrenquelle im Zusammenhang mit strittigen Drittanbieterforderungen eingestuft, da sie ganz eigene wirtschaftliche Interessen in diesem Nutzungsablauf besitzen. **Affiliates** werden in

60 Affiliates sind „Vertriebspartner“ für einen Anbieter, die Werbemittel auf ihrer Webseite einbauen. Das können neben gewerblichen Webseitenbetreibern auch Privatpersonen sein. Zur weiteren Erklärung siehe Glossar.

61 Auch Mobile Network Operator (MNO) genannt.

technischer und finanzieller Hinsicht über **Affiliate-Netzwerke** organisiert.[62] Das Angebot eines **Drittanbieters** wird schließlich auf einer normalen Webseite präsentiert und kann unter anderem ein Video-on-Demand-Portal oder ein Spieleportal sein. Die Webseite wird entweder selbst unterhalten, denkbar ist aber auch, dass die technische Infrastruktur der **Aggregatoren** verwendet oder über ein **Affiliate-Netzwerk** bereitgestellt wird.

Die **Aggregatoren**, alternativ auch **Billing-Carrier** genannt, zu denen Unternehmen wie DIMOCO Germany GmbH, die net mobile AG oder die mobile business engine GmbH zählen, haben in diesem Nutzungsablauf mehrere Funktionen. Einerseits realisieren sie die Anbindung von Bezahllösungen hin zu den Telekommunikationsunternehmen und wickeln den eigentlichen Buchungsprozess der Drittanbieterleistung über eine eigene technische Infrastruktur ab. Drittanbieter müssen sich derzeit in der Regel an die Aggregatoren wenden, um überhaupt Leistungen über die Mobilfunkrechnungen der Telekommunikationsbetreiber abwickeln zu können. Andererseits übernehmen die Aggregatoren die Administration und Organisation der Drittanbieter gegenüber den Telekommunikationsunternehmen. Außerdem müssen Drittanbieter mit Sitz im Ausland gemäß § 45p Abs. 1 Telekommunikationsgsetz (TKG) einen allgemeinen Zustellungsbevollmächtigten im Inland angeben. Diese Funktion wird häufig durch die Aggregatoren wahrgenommen. Damit tauchen diese Unternehmen, zum Beispiel durch eine E-Mail-Adresse oder eine Hotline-Nummer, teilweise auch auf der Mobilfunkrechnung auf. Zudem unterhalten einige Aggregatoren im Sinne eines „One-Stop-Shops“ eigene Affiliate-Netzwerke und stehen somit zumindest auf dieser Ebene direkt mit den Affiliates in Beziehung.[63] Die **Mobilfunknetzbetreiber**, also Telekom, Vodafone oder Telefónica, bilden zumeist den Abschluss in dieser Kette. Sie betreiben das eigentliche Mobilfunknetz und stellen selbst die Rechnung über angefallene Leistungen an den Kunden oder veräußern diese an den Mobilfunkprovider, der in einem direkten Vertragsverhältnis mit dem Endkunden steht.

Marktmechanismen

Werden die dargestellten Abläufe betrachtet, stellt sich die Frage nach den monetären Flüssen zwischen den einzelnen Marktteilnehmern. Basierend auf zahlreichen Gesprächen mit Vertretern der beteiligten Akteure handelt es sich hierbei um eine Forderungsankaufkette, die nach dem Prinzip des Factorings[64] abläuft. Vereinfacht ausgedrückt bedeutet dies, dass der Drittanbieter seine Forderung gegenüber dem Mobilfunkkunden an den Aggregator verkauft, dieser wiederum an den Netzbetreiber oder den Mobilfunkprovider, der diese Forderung dann abschließend dem Kunden in Rechnung stellt.[65]

Im Zusammenhang mit netzunabhängigen Mobilfunkprovidern, wie zum Beispiel mobilcom-debitel, ist diese Forderungsankaufkette bis zum Kunden jedoch nicht ganz eindeutig, da der Aggregator den Mobilfunknutzer erst einmal nicht kennt, sondern nur einem Netzbetreiber zuordnen kann, welcher wiederum nicht mit dem Nutzer in einer Vertragsbeziehung steht. Für den Kunden ist die konkrete Abrechnungskette nicht erkennbar, da der Betrag, wie vom Diensteanbieter angegeben, letztlich mit den Anbieterdaten auf der Mobilfunkrechnung seines Mobilfunkproviders ausgewiesen wird.[66]

Die einzelnen Marktteilnehmer erhalten in Abhängigkeit von dem Inhalt, welcher angeboten wird, unterschiedlich hohe Anteile des jeweiligen Transaktionsvolumens. Die Kosten für den Ankauf der Forderungen der Netzbetreiber orientieren sich dabei auch an der Höhe des Ausfallrisikos der Forderung. So sind Ticketbuchungen im öffentlichen Nahverkehr oder redaktioneller Inhaltserwerb bei einem bekannten Medienhaus deutlich geringer provisioniert als Inhalte aus dem Erotiksegment. Darüber hinaus spielt nach Aussage der Netzbetreiber auch die Stärke des Wettbewerbs alternativer Bezahlverfahren bei den einzelnen Drittanbieterangeboten eine wesentliche Rolle.[67]

Neben dieser eindeutigen Wertschöpfungskette stehen die Umsätze von Affiliates und Affiliate-Netzwerken. Je nach Anbieter verdienen Affiliates „während der gesamten Laufzeit eines Abos“ mit.[68] Erlöse derartiger

62 Siehe auch 2.3.

63 Siehe NTH Group (2015), Moneyhouse AG (2017) und Net Mobile AG (2016).

64 Factoring ist der laufende Ankauf von Forderungen aus Lieferungen oder Leistungen des Factoringkunden (= „Anschlusskunden“ oder „Verkäufers“) durch den Factor („Käufer“) nach Maßgabe eines Rahmenvertrags. Je nach vertraglicher Ausgestaltung kann der Anschlusskunde dabei dem Factor die gesamte Debitorenbuchhaltung, einschließlich des Inkasso- und Mahnwesens und des gerichtlichen Forderungseinzugs, übertragen. [Bundesanstalt für Finanzdienstleistungsaufsicht (2009)].

65 Zur rechtlichen Bewertung des Factorings in diesem Zusammenhang, siehe Kapitel 4.2.

66 Stellungnahme Clean Market Initiative, 25.11.2016.

67 Vgl. ebda.

68 Siehe W2M GmbH (2016).

15 EINHEITLICHER BEZAHLPROZESS DER CLEAN-MARKET INITIATIVE

Schritt 1: Der Verbraucher gibt seine MSISDN in die Maske ein.

Schritt 2: Der Verbraucher gibt die ihm zugesandte TAN in die Maske ein.

Quelle: mdk Gesellschaft für Entwicklung und Betrieb technischer Mehrwertdiensteplattformen mbH

Kampagnen, Zielgruppen und gewünschte Endgeräte werden teilweise im Internet auf speziellen Portalen veröffentlicht. Medienberichten zufolge sind einige Drittanbieterangebote von den Eigentumsverhältnissen her bestimmten Aggregatoren zuzuordnen.[69] Damit können die Anteile des Transaktionsvolumens im Rahmen eines Drittanbieterabonnements von Drittanbieter, Affiliate-Netzwerk und Aggregator in eine Hand fallen.

4.2 DIE CLEAN MARKET INITIATIVE[70] DER MOBILFUNKUNTERNEHMEN

Die hohe Anzahl der Kundenbeschwerden im Zusammenhang mit der Abrechnung von Drittanbieterleistungen über die Mobilfunkrechnung hat zur Gründung der Clean Market Initiative im Jahre 2011 geführt. Zu deren Initiatoren zählen Telefónica Germany, Telekom Deutschland und Vodafone; mobilcom-debitel hat sich 2012 der Initiative angeschlossen. [71]

Konkret drückte sich die Initiative in der Einführung verbindlicher Gestaltungsregeln des Bezahlablaufs für Abos im Internet aus, um die geforderte Button-Lösung rechtskonform umzusetzen.[72] Diese von allen Mobilfunkanbietern entwickelte und übernommene Bezahlmaske soll die Kosten, Laufzeiten und Kündigungsmöglichkeiten klar aufschlüsseln und damit „ein standardisiertes Bestellverfahren“[73] etablieren. Bei allen Abonnements sei außerdem eine zweite Zustimmung per „Button-Klick“ notwendig, welche zusätzliche Sicherheit für den Verbraucher schaffen sollte.[74]

Für die Web-Billing-Variante des Bezahlverfahrens stellt sich die Vorlage wie in Abbildung 15 dar.[75]

In den Folgejahren wurden die Vorgaben verfeinert (mobiles Template, Konfigurator etc.) und an neue rechtliche Rahmenbedingungen angepasst. Darüber hinaus wurde

69 Siehe Rosenthal (2017).

70 Sofern auf Aussagen der Clean Market Initiative verwiesen wird, ist damit eine gemeinsame Position aller an dieser Initiative beteiligten Unternehmen gemeint.

71 Siehe Präsentation der Clean Market Initiative vom 30.08.2016.

72 Siehe auch § 312j BGB, insbesondere Abs. 3: „Der Unternehmer hat die Bestellsituation bei einem Vertrag nach Absatz 2 so zu gestalten, dass der Verbraucher mit seiner Bestellung ausdrücklich bestätigt, dass er sich zu einer Zahlung verpflichtet. Erfolgt die Bestellung über eine Schaltfläche, ist die Pflicht des Unternehmers aus Satz 1 nur erfüllt, wenn diese Schaltfläche gut lesbar mit nichts anderem als den Wörtern „zahlungspflichtig bestellen“ oder mit einer entsprechenden eindeutigen Formulierung beschriftet ist.“

73 Siehe mdk GmbH (2016a).

74 Siehe mdk GmbH (2016a).

75 Die Vorgaben zur optischen Umsetzung des Direct Billing-Verfahrens sind nach Aussage der Mobilfunkunternehmen identisch, Differenzen ergeben sich nur in der funktionalen Ausgestaltung der Formularfelder und Buttons. Siehe mdk GmbH (2016b).

eine kontinuierliche Marktbeobachtung eingeführt sowie ein Erfahrungsaustausch der MNOs im Sinne eines Roundtables etabliert.[76]

Seit 2015 wird nun die Einführung des sogenannten MNO-Redirects vorangetrieben, der den Bestellprozess für Endkunden um ein Element ergänzt und diesen auf der technischen Infrastruktur der MNOs umsetzt (siehe auch Kapitel 4.3).

Drittanbieter und deren Angebote müssen ein Freischaltungs- und Prüfverfahren bei den Netzbetreibern durchlaufen, bevor diese Leistungen über die Mobilfunkrechnung abgerechnet werden können. Das entsprechende Verfahren wird nachfolgend skizziert.

Organisation, Prüfung und Technische Freischaltung

Telekom, Telefónica und Vodafone haben ein webbasiertes System initiiert und konzipiert, welches einerseits zur Organisation fast aller Drittanbieter, andererseits als Basis für Tests von deren Angeboten verwendet wird. Dieses System ist seit Anfang 2014 im Einsatz und wird von dem extern beauftragten Unternehmen mdk GmbH entwickelt und betrieben. Über das System werden circa 50 Aggregatoren sowie mehr als 1.000 Drittanbieter beziehungsweise Dienste-Erbringer und deren Leistungen organisiert. mobilcom-debitel ist nicht an dieses webbasierte System angeschlossen, sondern führt die Anbieter- bzw. Dienstanmeldung in einem separaten Prozess durch, der allerdings auf den gleichen Prüfungskriterien aufsetzt und auf Zulieferung der entsprechenden Informationen basiert.[77]

Die Voraussetzung zur Nutzung dieser Webplattform ist eine Vertragsbeziehung zwischen Aggregator und Telekommunikationsunternehmen. In einem ersten Schritt erfolgt die Prüfung und Freischaltung der Drittanbieter. Dazu werden die Unternehmensdaten, beispielsweise Adressdaten und Umsatzsteueridentifikationsnummer, durch den Aggregator im System erfasst. Weiter muss eine Abtretungserklärung für anfallende Forderungen von Seiten des Drittanbieters in das System geladen werden. Die Erfassung und Anmeldung eines Drittanbieters, dessen Sitz sich nicht in Deutschland befindet, erfolgt ausschließlich dann, wenn ein Zustellungsbevollmächtigter in Deutschland nachgewiesen wurde und die entsprechenden Kontaktinformationen des Kundenservices für Verbraucher vorliegen. Sind die Daten vollständig, dann schaltet der Aggregator den Drittanbieter zur Prüfung durch die gewünschten Mobilfunkanbieter frei, auf deren Rechnung der Drittanbieter erscheinen soll.

Die Überprüfungsintensität von deren Seiten hängt dabei von der eigenen Einschätzung hinsichtlich der Seriosität der Drittanbieter ab. Laut Clean Market Initiative zählen einerseits formale Aspekte wie Adressdaten des Unternehmens, der Handelsregistereintrag inklusive verantwortlicher Personen zu den Prüfkriterien. Im Bedarfsfall nehmen die MNO weitergehende Prüfungen vor, die sich beispielsweise auf die Nationalität des Leistungserbringers beziehen sowie auf eventuelle Negativbewertungen durch externe Agenturen oder andere Ressourcen (zum Beispiel auf Grund von Auffälligkeiten von früheren Geschäftsbeziehungen und Dienstetests).[78]

Hat das Telekommunikationsunternehmen den Drittanbieter aktiviert, erfolgt in einem zweiten Schritt die Prüfung der entsprechenden Leistungen (Services). Diese werden analog zum vorangegangenen Schritt von den Aggregatoren erfasst und dem Drittanbieter zugewiesen. Zu den Daten zählen unter anderem die URL, über welche das Angebot erreichbar ist, sowie Angaben zum Preis des Angebotes und das Abrechnungsintervall. Anschließend wird die Leistung vom Aggregator wiederum zur Prüfung durch die gewünschten Mobilfunkanbieter freigegeben. Diese berücksichtigen, eigenen Aussagen zur Folge, bei ihren Tests auch qualitative Aspekte wie die inhaltliche Art des Angebotes und die Einstiegsseite des Dienstes. Einschätzungen in Bezug auf die Kosten des Angebotes, insbesondere hinsichtlich Preisspanne oder Preispunkte, und das Abrechnungsintervall spielen dabei ebenso eine Rolle wie die Nachhaltigkeit des Angebotes oder das Leistungsversprechen.[79]

Anschließend übernehmen die Mobilfunkunternehmen die eingegebenen Daten für die eigene Buchungsplattform und geben die Leistung „kommerziell“ frei. Daraufhin wird die Leistung von dem jeweiligen Unternehmen technisch überprüft. Ist das Resultat positiv, wird der Dienst aktiviert.

76 Siehe Präsentation der Clean Market Initiative vom 30.08.2016.
77 Stand: 2016.
78 Siehe Stellungnahme der Clean Market Initiative, 25.11.2016.
79 Siehe ebda.

Von den vorgenannten eher qualitativen Freischaltungsprozessen zu unterscheiden ist die technische Aktivierung der Drittanbieterleistungen für den eigentlichen Abrechnungsprozess. Diese findet über die eigenen Billing-Systeme des jeweiligen Mobilfunkanbieters statt, wenn Dienst und Anbieter die qualitativen Prüfungen bestanden haben.

Tests der Drittanbieterdienste durch die Mobilfunkanbieter

Um die vertraglichen Vorgaben (insbesondere zum Bestell- und Bezahlvorgang) bei den Drittanbietern auch nach der Freischaltung zu überprüfen, ist ein Kontrollverfahren von Seiten der Mobilfunkanbieter installiert worden, das von der mdk GmbH durchgeführt wird. Diese kontinuierlich – auch außerhalb der üblichen Bürozeiten – durchgeführten stichprobenartigen Qualitätskontrollen haben einen monatlichen Umfang von rund 250 Stück. Sie umfassen einen Internetnutzungsvorgang, zum Teil vom Klicken auf einen Werbebanner über die eigentliche Nutzung des Angebotes bis hin zur Buchung des Abos/der Dienstleistung. Die Ergebnisse werden via Screenshot und textlichen Anmerkungen festgehalten.

Die eigentlichen Testkriterien werden durch die einzelnen MNOs vorgegeben und basieren laut Clean Market Initiative auf dem jeweiligen Vertrag mit dem Aggregator, gesetzlichen Vorgaben sowie festgelegten Details aus dem vorhergehenden Freischaltungsprozess. Darüber hinaus fließen Vorgaben aus dem oben genannten Styleguide, technische Spezifikationen der Netzbetreiber-Schnittstellen sowie unter Umständen Rückmeldungen aus den Rechtsabteilungen und Kundenservicebereichen der jeweiligen MNO in die Prüfkriterien ein, die kontinuierlich an aktuelle Marktentwicklungen angepasst werden. Die Ergebnisse der Tests werden wöchentlich zwischen der mdk GmbH und den Netzbetreibern ausgetauscht.[80]

Fällt ein Anbieter durch die Nichteinhaltung des Regelwerks auf, erfolgt eine Meldung an die betroffenen MNO, die für derartige Fälle unterschiedliche Eskalationsstufen vorhalten. Die höchste Eskalationsstufe besteht in einer Kündigung der Geschäftsbeziehung, die nach Aussagen der Mobilfunkunternehmen auch wahrgenommen werden.

Neben den externen Dienstetests durch die mdk, überprüfen auch die Telekommunikationsunternehmen die Drittanbieter und ihre Services. Die Überprüfung bezieht sich dabei sowohl auf die Bestandsservices als auch auf neu angemeldete Dienste.

Bestandsservices werden vorrangig an Hand von Rückmeldungen aus den Kundenservicebereichen und der täglichen Umsatzentwicklung begutachtet. Ein weiteres ausschlaggebendes Kriterium stellt für die Telekommunikationsunternehmen nach eigenen Aussagen die transparente Kommunikation des Leistungsangebotes dar.[81]

4.3 REDIRECT

Um Kunden nun besser vor potentiellem Missbrauch im Drittanbietermarkt zu schützen, wurde vor allem im Laufe des Jahres 2016 eine Neuerung im Buchungsprozess eingeführt: Der Redirect, der bei mobilen Internetsitzungen eingesetzt werden kann.

Für den Verbraucher äußert sich der Redirect in einer Weiterleitung von der Webseite des Drittanbieters, auf der das Angebot präsentiert wird, hin zu einer Bezahlseite, die sich optisch eindeutig von der vorherigen Seite unterscheidet. Diese Bezahlseite ist zum Teil im Corporate Design des jeweiligen Telekommunikationsunternehmens gehalten und liegt auch auf deren technischer Infrastruktur.

Der konkrete Einsatz des Redirect-Verfahrens kann zwischen den einzelnen Telekommunikationsunternehmen unterschiedlich ausfallen. Konsens herrscht darüber, dass „nach individueller Risikobewertung (…) insbesondere solche Anbieter mit einer sehr anspruchsvollen Nutzer-Erfahrung in Verbindung mit einem erfahrungsgemäß geringen Missbrauchspotential wie zum Beispiel Apple, ÖPNV, Spotify, Axel Springer, Netflix, Google etc. und „closed-community“-Diensten [vom Redirect-Verfahren] ausgenommen werden [können].“[82] Das erklärte Ziel beim Einsatz des Redirect-Verfahrens ist es, „eine maximale Transparenz für den Endkunden im Abo-Geschäftsmodell zu gewährleisten, um so Beschwerden und zusätzliche Endkundenanfragen weitestgehend zu verhindern. Dies ist insbesondere außerhalb von sog.

80 Siehe Stellungnahme der Clean Market Initiative, 25.11.2016.

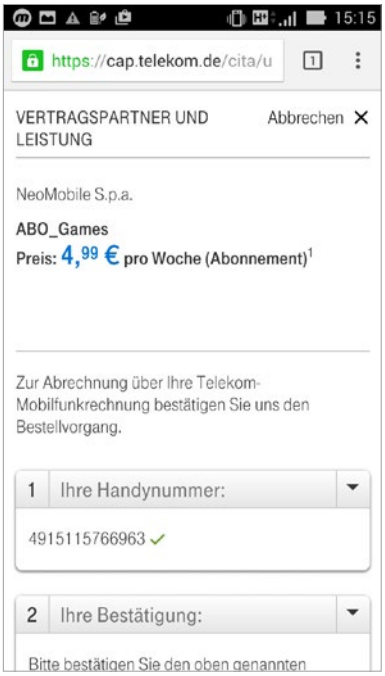
81 Siehe Stellungnahme der Clean Market Initiative, 25.11.2016.

82 Stellungnahme der Clean Market Initiative, 25.11.2016.

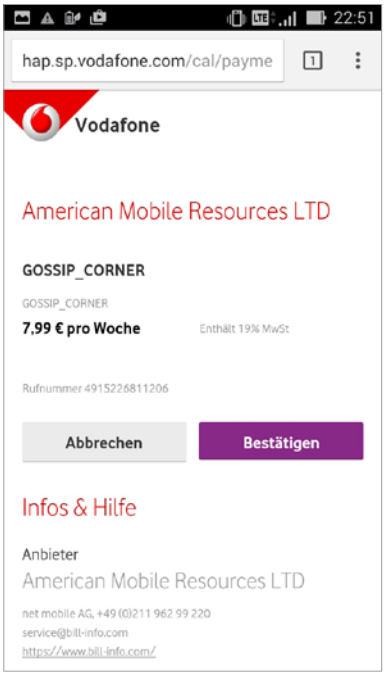
16 REDIRECT-BEZAHLSEITEN IM VERGLEICH

Telefónica

Telekom



Vodafone



Quelle: Telefónica Germany GmbH & Co. OHG (Dezember 2016), Telekom Deutschland GmbH (Dezember 2016), Vodafone GmbH (Dezember 2016)

closed-community groups relevant, bei denen der Kunde vor einem Kauf keine separate Registrierung durchführen muss. Hierzu zählen derzeit insbesondere Dienste im Bereich Erotik oder Handycontent, für die das Redirect-Verfahren zum Einsatz kommt."[83]

Durch diesen Redirect können die Mobilfunkanbieter einerseits die optische und rechtliche Ausgestaltung der eigentlichen Buchungsseite allein verantworten, wie zum Beispiel die Umsetzung der Button-Lösung. Darüber hinaus können die für das Prüfprotokoll notwendigen Daten, die im strittigen Fall vorgelegt werden müssen, von der eigenen technischen Infrastruktur abgenommen werden.

Die Redirect-Lösungen der einzelnen Anbieter unterscheiden sich sowohl im Ablauf als auch in ihrer technischen Ausgestaltung. Darüber hinaus zeigt sich zum Zeitpunkt der Untersuchung auch eine unterschiedliche juristische Auffassung bezüglich des Zeitpunktes eines Vertragsschlusses.[84,85] Zum Teil kommen auch noch bestimmte Spezifika der Aggregatoren oder Drittanbieter zum Einsatz, so dass sich der Ablauf in Details unterscheiden kann, beispielsweise auch in Bezug auf den Versand von SMS-Bestätigungen.[86]

Alle hier betrachteten Redirect-Bezahlseiten enthalten zumindest folgende Informationen

- Anbieter des Dienstes
- Name des Dienstes
- Kosten des Dienstes
- Intervall des Berechnungszeitraums
- Die zugreifende Mobilfunknummer

83 Stellungnahme der Clean Market Initiative, 25.11.2016.

84 Hierzu sind die MNO bestrebt, eine einheitliche, harmonisierte Rechtsaufassung und somit einen einheitlichen Standardablauf zu erreichen.

85 Zur weiteren Diskussion siehe auch Kapitel 5.4

86 Zur Ausgestaltung der SMS-Bestätigung, siehe S. 18 ff.

17 TECHNISCH FLÄCHENDECKEND MÖGLICHER EINSATZ DES REDIRECT VERFAHRENS[a]

	Prepaid		Postpaid	
	Einzelkauf	Abo	Einzelkauf	Abo
mobilcom-debitel	siehe Netzbetreiber		Januar 2017	
Telefónica (Netzbetreiber)	Im Einsatz (kein Zeitpunkt bekannt)			
Telekom (Netzbetreiber)	Im Einsatz seit August 2016			
Vodafone (Netzbetreiber)	Im Einsatz seit Juli 2016			

a Der konkrete Einsatz des Redirect-Verfahrens bei einem Drittanbieterangebot erfolgt in Abhängigkeit der individuellen Bewertung durch den Netzbetreiber (siehe oben).

- Buttons zum Bestätigen des Vorgangs
- Buttons zum Abbrechen des Vorgangs
- Textliche Informationen zum Bezahlen über die Mobilfunkrechnung

Verlinkungen auf das Impressum finden sich hingegen nur bei Telefónica und der Telekom, eine Verlinkung zu den AGB wiederum nur bei Telefónica und Vodafone, wobei dies bei letzterem nicht eindeutig ersichtlich ist. Ein Hinweis auf einen „Widerruf“ kommt nur bei Telefónica vor und umfangreiche Anbieterinformationen nur bei Vodafone.

Allen Redirect-Lösungen gemein ist aber, dass dritte Leistungserbringer oder Aggregatoren keine Bestellung bzw. Abbuchung des Betrages auf den Abrechnungssystemen der Netzbetreiber auslösen können, wenn der Kunde auf der Redirect-Seite den Vorgang nicht durch Betätigen des dortigen Buttons abschließt. Einzig das Postpaid-Segment von mobilcom-debitel bildete zum Zeitpunkt der Untersuchung eine Ausnahme von der beschriebenen technischen Umsetzung. Der Prepaidbereich des Unternehmens wurde hingegen bereits durch die Redirect-Seiten der einzelnen Netzbetreiber geschützt.

In Bezug auf die eigenen Tochterunternehmen stellt sich der Einsatz des Redirect-Verfahrens weitestgehend einheitlich dar, nur in Einzelfällen gibt es Ausnahmen.

Bei Telefónica wird das Verfahren unabhängig von der Marke eingesetzt. Die konkrete Ausgestaltung unterscheidet sich nur in der Kundenansprache auf der Redirect Seite, dazu zählt auch die optische Darstellung.

Vodafone differenziert bei seinen Tochterunternehmen grundsätzlich nicht in der Anwendung des Verfahrens. Aus abrechnungstechnischen Gründen ist jedoch das Carrier Billing bei Otello derzeit noch nicht aktiviert, so dass auch kein Anlass für das Redirect-Verfahren besteht.

Bei der Telekom Deutschland und ihren Tochterunternehmen wird das Verfahren in der gleichen Ausprägung eingesetzt.

Bei mobilcom-debitel werden die Tochterunternehmen callmobile und klarmobil dahingehend anders behandelt, dass diese zu 100 Prozent über das Verfahren der Netzbetreiber (Telekom, Vodafone und Telefónica) geleitet werden.

4.4 ZUSAMMENFASSUNG DRITTANBIETERMARKT UND SICHERUNGSMECHANISMEN

Bis eine Drittanbieterleistung auf der Mobilfunkrechnung des Verbrauchers auftaucht, ist eine ganze Anzahl an Akteuren zwischengeschaltet, die auch monetär an der Transaktion beteiligt sind. Ausgehend von dem Drittanbieter, um dessen Leistung es geht, zählen werbetreibende Webseite-Betreiber (Affiliates) dazu, ebenso wie die Werbenetzwerke (Affiliate-Netzwerke), die Werbekampagnen organisieren und auf die Drittanbieterseiten weiterleiten. Die gebuchte Leistung wird vom

Drittanbieter über den Aggregator (oder Billing-Carrier) an den Netzbetreiber veräußert. Sofern dieser nicht der Vertragspartner des Verbrauchers ist, kommt noch der Mobilfunkprovider hinzu, welcher dem Verbraucher die Leistung in Rechnung stellt. Zu beobachten ist, dass teilweise unternehmerische Verflechtungen zwischen Drittanbieter, Affiliate-Netzwerk und Aggregatoren bestehen.

Die Übertragung der Leistung von einem Akteur zum anderen erfolgt nach dem Prinzip des Factorings, also einer Forderungsankaufkette. Zuletzt ist die Forderung im Besitz des Unternehmens, welches dem Verbraucher die Rechnung ausstellt.

Die einzelnen Marktteilnehmer erhalten unterschiedlich hohe Anteile des jeweiligen Transaktionsvolumens. Die Kosten für den Ankauf der Forderungen der Netzbetreiber orientieren sich dabei auch an der Höhe des Ausfallrisikos der Forderung sowie der Stärke des Wettbewerbs alternativer Bezahlverfahren bei den einzelnen Drittanbieterangeboten.

Der uneinheitliche Bestellablauf, dessen optische Ausgestaltung sowie eine hohe Anzahl an Kundenbeschwerden haben zur Gründung der Clean Market Initiative im Jahre 2011 geführt (Initiatoren: Telefónica Germany, Telekom Deutschland und Vodafone), welcher sich 2012 auch mobilcom-debitel anschloss. Seitdem wurde die Ausgestaltung des Bestellprozesses in weiten Teilen optisch vereinheitlicht sowie ein Organisations- und Prüfverfahren installiert, das Drittanbieter und deren Leistung zur Aufnahme qualifiziert und auch während des Betriebs wiederkehrende Tests vorsieht. Seit 2016 ist über das Redirect-Verfahren ein zusätzlicher Sicherungsmechanismus implementiert worden, der Kunden besser vor potentiellem Missbrauch im Drittanbietermarkt schützen soll.

5. RECHTLICHE ANALYSE DER DRITTANBIETERPROBLEMATIK

Für die Drittanbieterproblematik aus rechtlicher Sicht ist der Umstand wesentlich, dass Mobilfunkunternehmen Drittanbieterforderungen einziehen lassen. Diese Forderungen sind zwar auf der Telefonrechnung sichtbar; für die betroffenen Mobilfunkkunden allerdings nicht immer direkt nachvollziehbar.

Methodik zur rechtlichen Analyse

Im Zuge der Sonderuntersuchung wurde der Drittanbietermarkt durch das Referat Recht des Marktwächters Digitale Welt, Schwerpunkt Telekommunikationsdienstleistungen, der Verbraucherzentrale Schleswig-Holstein juristisch geprüft.

§ METHODIK ZUR RECHTLICHEN ANALYSE

Dieser Teil der Untersuchung betrachtet

- die rechtlichen Beziehungen zwischen den Beteiligten,
- die rechtliche Stellung des Mobilfunkkunden im Verhältnis zu den Beteiligten und
- den Ablauf des Bestellvorgangs einer Drittanbieterleistung.

Die Prüfung orientierte sich im Wesentlichen an den geltenden Vorschriften des

- Telekommunikationsgesetzes,
- Bürgerlichen Gesetzbuches,
- Telemediengesetz (TMG)

unter Einbeziehung neuester gesetzgeberischer Vorhaben sowie der einschlägigen Rechtsprechung.

5.1 ALLGEMEINE RECHTLICHE ASPEKTE

Einer rechtlichen Analyse gehen die Identifizierung beteiligter Akteure sowie deren Beziehung zueinander voraus. Wie in vorherigen Kapiteln bereits erläutert, setzt sich der Drittanbietermarkt unter anderem aus folgenden Parteien zusammen:

1. Mobilfunkkunde
2. Mobilfunkanbieter/-unternehmen, auch Teilnehmernetzbetreiber genannt[87]
3. Drittanbieter
4. Aggregator bzw. Billing-Carrier

5.1.1 Vertragsbeziehungen

Vor jeder Drittanbieterforderung steht das Schließen des Telekommunikationsvertrages zwischen Mobilfunkkunden und Mobilfunkunternehmen. Hierbei verpflichtet sich einerseits das Mobilfunkunternehmen dem Mobilfunkkunden den Zugang zum öffentlichen Telekommunikationsnetz zu eröffnen. Andererseits verpflichtet sich der Mobilfunkkunde zur Zahlung des hierfür vereinbarten Entgelts. Dieses wird wiederum über die Mobilfunkrechnung fakturiert, welche unter anderem der nachträglichen Kostenkontrolle dient. Der Telefondienstvertrag ist als Dauerschuldverhältnis zu qualifizieren.

Der geschlossene Telekommunikationsvertrag beinhaltet eine Vielzahl an vorformulierten Vertragsbedingungen[88]. Unter anderem wird dem Mobilfunkunternehmen das Recht eingeräumt, auch Forderungen über Drittanbieterleistungen vom Konto des Mobilfunkkunden einzuziehen. Dabei finden sich Formulierungen wie „Die vereinbarten Preise für Leistungen einschließlich sämtlicher Preise, zu denen congstar den Zugang vermittelt, werden von dem Guthaben des Kontos in Abzug gebracht.“[89], oder „Vodafone ist berechtigt, Entgelte für Verbindungen zu Diensteangeboten Dritter geltend zu machen, zu denen Vodafone die Verbindung herstellt.“[90].

Problematisch sind diese Vereinbarungen dann, wenn der Kunde die Abbuchung einer lediglich behaupteten Forderung **nicht durch bloßen Widerspruch verhindern** oder **rückgängig machen kann.** Derartige Vertragsbe-

87 Zur besseren Lesbarkeit wird statt des Rechtsbegriffs Teilnehmernetzbetreiber im Folgenden der Begriff Mobilfunkunternehmen verwendet, das sowohl der Netzbetreiber sein kann, aber auch ein Mobilfunkprovider.
88 Allgemeine Geschäftsbedingungen i.S.v. § 305 Abs. 1 BGB.
89 Congstar (2016), Stand AGB 29.06.2017, abgerufen am 01.08.2017.
90 Vodafone (2017), Stand AGB 1.10.2017, abgerufen am 01.08.2017.

dingungen sind für den Verbraucher unerwartet und verschieben die Beweislast zu seinem Nachteil.

Wenn das Mobilfunkunternehmen die Zahlung einer Forderung über Drittanbieterleistungen verlangt, dann ist es folglich auch verpflichtet, Einwendungen gegen sich gelten zu lassen. Der Schuldner kann dem neuen Gläubiger jene Einwendungen entgegenhalten, welche ursprünglich gegen den bisherigen Gläubiger galten.[91]

Da es sich bei diesen Zahlungsgeschäften um eine Forderungsankaufkette handelt, die nach dem Prinzip des Factorings funktioniert, müsste das Mobilfunkunternehmen zum Zeitpunkt der Rechnungsstellung Inhaber der Forderung sein. Aufgrund der Ausnahme in § 1 Abs. 10 Nr. 11 ZAG (Gesetz über die Beaufsichtigung von Zahlungsdiensten) sind diese Abläufe jedoch keine Zahlungsdienste, da die Netz- oder Systembetreiber, auch dem eigenen Selbstverständnis nach, nicht ausschließlich als zwischengeschaltete Stelle zwischen dem Zahlungsdienstnutzer, dem Mobilfunkkunden, und dem Lieferanten der Waren oder Dienstleistungen tätig sind. Damit sind diese Geschäfte im Vergleich zu anderen elektronischen Bezahlverfahren nicht aufsichtspflichtig.[92]

Der Mobilfunkkunde und der Aggregator (oder Verbindungsnetzbetreiber) wiederum stehen in keiner vertraglichen Beziehung. Der Aggregator ist nur als Hilfsperson zu verstehen, deren Beitrag zur Erbringung der Drittanbieterleistung notwendig ist.

Zwischen dem Mobilfunkkunden und dem Drittanbieter wird (in der Regel via Smartphone) ein Vertrag über die Mehrwertdienstleistung geschlossen. Damit verpflichtet sich der Drittanbieter zur Erbringung der Mehrwertdienstleistung, der Mobilfunkkunde verpflichtet sich wiederum zur Zahlung des vereinbarten Entgelts.

5.1.2 Vertrag über Mehrwertdienste

Ein Vertrag über Mehrwertdienste setzt sich aus einem Telekommunikationsdienst[93] sowie einer weiteren Dienstleistung zusammen.[94] Bei einem Vertragsschluss über Drittanbieterleistungen kommt der Vertrag durch Angebot und Annahme[95] zustande. Hat der Mobilfunkkunde jedoch gar nicht die Absicht, in ein Vertragsverhältnis mit dem Drittanbieter zu treten und möchte einzig ein „Pop-up“ auf dem Bildschirm wegklicken, dann liegt folglich auch keine auf Vertragsabschluss gerichtete Willenserklärung vor.

Werden außerdem die Kosten des Drittanbieterdienstes im Fließtext versteckt, dann ist diese Formulierung überraschend, weil sie vom Kunden an dieser Stelle nicht erwartet wird.[96] Der bloße Klick auf eine Schaltfläche entspricht auch keinem wirksamen Abschluss eines kostenpflichtigen Vertrags, da nicht nachgewiesen werden kann, dass der Mobilfunkkunde den Vertrag unter den tatsächlichen Bedingungen abschließen möchte.[97]

Hinzu kommt, dass die für einen Vertragsabschluss im elektronischen Rechtsverkehr geschaffenen gesetzlichen Mindestvoraussetzungen vorliegen müssen. In jedem Fall erforderlich sind dabei die Belehrung über bestehende Widerrufsrechte sowie die sogenannte „Buttonlösung“.

Grundsätzlich gilt: Ein **Widerrufsrecht**[98] besteht auch beim Download von digitalen Inhalten.[99] Dieses erlischt erst, wenn der Drittanbieter die Dienstleistung vollständig erbracht hat und wenn dieser erst damit begonnen hat, nachdem der Verbraucher mit seiner Zustimmung bestätigt, von dem Verlust des Widerrufsrechts Kenntnis genommen zu haben.[100] Das entspricht auch der Absicht des Erwägungsgrunds Nr. 39 Richtlinie 2011/83/EU (Verbraucherrechterichtlinie), „Abo-Fallen“ zu verhindern. Der Download darf also erst beginnen, wenn die genannten Voraussetzungen definitiv vorliegen. Bei nicht ordnungsgemäßer Belehrung endet das Widerrufsrecht spätestens 12 Monate und 14 Tage nach Vertragsschluss.

Die im Jahr 2012 geschaffene **Buttonlösung** verpflichtet Drittanbieter, die genauen Vertragskonditionen[101] klar und verständlich in hervorgehobener Weise zur Verfügung zu stellen. Dies muss vor dem Kauf des Dienstes geschehen. Ziel der Buttonlösung ist, dass der Verbrau-

91 So auch LG Potsdam U v 26.11.2015, Az.: 2 O 340/14.
92 Siehe Stellungnahme Clean Market Initiative, 25.11.2016 & BaFin (2016).
93 I.S.d. § 3 Nr. 24 TKG.
94 Vgl. Ditscheid/Rudloff, Vorbemerkung zu § 6 a TKG Rn. 1. in Geppert (2013).
95 I.S.d. §§ 145 ff. BGB.
96 Siehe LG Berlin, U. v. 21.10.2011, Az. 50 S 143/10.
97 Siehe Kapitel 2.3.
98 Gem. §§ 355, 356 BGB.
99 Gem. § 312g Abs. 1 BGB.
100 Gem. § 356 Abs. 4 BGB.
101 Gem. § 312j Abs. 2 BGB von Artikel 246a § 1 Absatz 1 Satz 1 Nummer 1, 4, 5, 11 und 12 EGBGB.

cher vor der Bestellung weiß, worauf er sich einlässt und er demnach ausdrücklich bestätigt, dass er sich zu der vereinbarten Zahlung verpflichtet.[102] Um Missverständnisse zu vermeiden, muss der Anbieter für den finalen Kaufbutton eine eindeutige Formulierung wie „zahlungspflichtig bestellen“ wählen.[103] Nur so ist der Kaufvertrag auch tatsächlich wirksam. Beschriftet der Anbieter den finalen Kaufbutton lediglich mit „jetzt anmelden“, „weiter“ oder „bestellen“, dann kommt er seiner Pflicht der Buttonlösung nicht nach, da er den Verbraucher nicht ausreichend auf die Zahlungspflicht hinweist. Um die bestmögliche Übersichtlichkeit zu gewährleisten, darf der Kaufbutton keine weiteren Informationen enthalten, wobei auch die Verwendung eines Euro-Symbols unzulässig ist.

Ebenso verhält es sich mit vorerst kostenfreien Leistungen, welche zu einem späteren Zeitpunkt automatisch kostenpflichtig werden. Beschriftungen wie „jetzt kostenlos testen“ oder „jetzt gratis testen – danach kostenpflichtig“ sind unzureichend und demnach unzulässig. Klickt der Verbraucher lediglich ein „Pop-up“ weg, dann ist die Buttonlösung nicht eingehalten. Besteht eine Forderung gegenüber einem Mobilfunkkunden, dann hat der Drittanbieter den Nachweis über die Einhaltung der Buttonlösung zu führen. Folglich: In einem Fall von Nichteinhaltung der Buttonlösung ist aus rechtlicher Sicht keiner der beiden Parteien zur Leistung verpflichtet.[104]

5.1.3 Rechte des Verbrauchers bei unberechtigten Forderungen

Aufgrund der technischen Infrastruktur ist es Drittanbietern möglich, nicht nur berechtigte sondern auch unberechtigte Forderungen gegen den Mobilfunkkunden geltend zu machen und die Einziehung des Rechnungsbetrages durch das Mobilfunkunternehmen zu veranlassen. Das Mobilfunkunternehmen, das das Recht hat, auf das Konto des Mobilfunkkunden zuzugreifen, wäre es auf der anderen Seite daher auch zuzumuten, den fordernden Drittanbieter mindestens anlassbezogen zu prüfen und zu überwachen, um den maximalen Schutz des Verbrauchers zu gewährleisten. Diese Prüf- und Überwachungspflichten können beispielsweise die Einhaltung der Buttonlösung, aber auch die ordnungsgemäße Belehrung über das Widerrufsrecht umfassen. Anderenfalls kann sich das Mobilfunkunternehmen durchaus schadensersatzpflichtig machen.

Hingegen existieren zum Schutz vor überzogenen Forderungen durch Drittanbieter keine gesetzlichen Regelungen wie beispielsweise die im Telekommunikationsgesetz geregelten Preishöchstgrenzen für die Bereiche Rufnummern, Premium- und Service-Dienste.[105]

Im Falle von nachweislichem Betrug[106] beziehungsweise Computerbetrug[107] kann der Mobilfunkkunde deliktische Schadensersatzansprüche gegen den Drittanbieter geltend machen, also Schadensersatzansprüche aufgrund eines Delikts. Voraussetzung hierfür ist allerdings ein beweisbar vorsätzliches Handeln sowie die Absicht rechtswidriger Bereicherung des Drittanbieters. Wird eine Forderung rechtsgrundlos eingezogen, dann hat der Mobilfunkkunde ein Recht auf Erstattung.[108]

Zu einer solchen unberechtigten Forderung kann es beispielsweise mittels Clickjacking kommen. Die Forderung des Drittanbieters entsteht also dadurch, dass der Mobilfunkkunde auf eine manipulierte Schaltfläche klickt, welche einen Mechanismus zur Überweisung eines Geldbetrages auslöst. Auch hier hat der Mobilfunkkunde das Recht, Rückzahlung, ggf. auch Schadensersatzansprüche vom Drittanbieter zu fordern.[109]

5.2 VOREINGESTELLTE DRITTANBIETERSPERRE

Mit dem Recht auf eine sogenannte Drittanbietersperre[110], also eine grundsätzliche Zugriffsverweigerung für Drittanbieter auf das mobile Endgerät des Mobilfunkkunden, besteht die Möglichkeit, unrechtmäßige Forderungen effektiv zu vermeiden. Diese Sperre muss der Mobilfunkkunde derzeit allerdings eigeninitiativ durch seinen Mobilfunkanbieter einrichten lassen. Ignoriert der Mobilfunkanbieter das Recht des Kunden auf eine Drittanbietersperre, dann muss er selbst für entstehende Schäden haften.[111]

102 Gem. § 312j Abs. 3 S. 2 BGB.
103 Gem. § 312j Abs. 3 S. 2 BGB.
104 So auch Art. 8 Abs. 2 der Verbraucherrechterichtlinie.
105 Gem. § 66d TKG.
106 Gem. § 263 StGB.
107 Gem. § 263a StGB.
108 Gem. § 812 Abs. 1 S.1 Alt. 2 BGB.
109 Gem. § 823 Abs. 2 i.V.m. § 263a StGB oder § 263 StGB.
110 Gem. § 45d Abs. 3 TKG.
111 Siehe Spindler und Schuster (2015), TKG § 45d Rn. 10.

Problematisch hierbei ist allerdings, dass der Kunde womöglich erst einen Anlass zum Schutz vor rechtswidrigen Drittanbieterforderungen sieht, wenn er negative Erfahrungen damit gemacht hat, also: wenn bereits ein Schaden bei ihm vorliegt. Nur eine voreingestellte, gegebenenfalls auch selektive Drittanbietersperre würde den Mobilfunkkunden vorsorglich vor negativen Drittanbietererfahrungen und -abrechnungen schützen. Der Mobilfunkkunde könnte bei einer selektiven Drittanbietersperre, die teilweise auch von den Mobilfunkunternehmen angeboten wird, selbst und ganz bewusst entscheiden, ob und welche Anbieter von dieser Sperre ausgenommen werden. Mit dieser Sensibilisierung für mögliche Gefahren erhält der Mobilfunkkunde gleichzeitig auch eine vollständige Kostenkontrolle.

5.3 GESAMTRECHNUNG

Damit ein Betrag vom Konto des Mobilfunkkunden eingezogen werden kann, ist es notwendig, dass das mobile Endgerät des Verbrauchers mit dem Internet verbunden ist. Über WAP- oder HTML-Protokolle kann bei einer Mobilfunkverbindung die der SIM-Karte zugeordnete MSISDN (Mobilfunkrufnummer) an den Drittanbieter übermittelt werden. Hiermit identifiziert der Mobilfunkanbieter den Mobilfunkkunden mittels der für den Mobilfunkvertrag hinterlegten Daten.

Ohne diesen „technischen Support“ des Mobilfunkanbieters ist die Abrechnung der Drittanbieterleistung nicht möglich. Eine Unterscheidung oder gar Prüfung der Berechtigung der Forderung kann in diesem automatisierten Vorgang ohne zusätzliches Sicherheitselement nicht erfolgen. Da dies im weiteren Ablauf automatisch in einem Zugriff auf das Vermögen des Mobilfunkkunden endet, ist diese Praxis kritisch zu hinterfragen.

5.3.1 Vergleich: Postpayment und Prepaid

Im Postpaid-Bereich erstellt der Anbieter eine Rechnung über angefallene Entgelte. Werden dem Mobilfunkkunden auch Leistungen Dritter berechnet, dann ist der Anbieter verpflichtet, diese Kosten in der Gesamtrechnung nach gesetzlichen Vorgaben aufzuschlüsseln.[112]

Im Gegensatz zum Postpayment wird bei Prepaidverträgen üblicherweise keine Rechnung ausgestellt.[113] Außerdem besteht kein Anspruch auf einen Einzelverbindungsnachweis[114], also nach Einzelverbindungen aufgeschlüsselte Rechnungen zur detaillierten Kostenkontrolle. Sofern das Telekommunikationsunternehmen seinen Prepaidkunden auch sonst keine Möglichkeit bietet, beispielsweise über Onlinekundenportale ihre Kostenaufstellung einzusehen, ist eine Transparenz bezüglich berechneter Drittanbieterleistungen in diesem Fall nicht gegeben. Denn: Prepaidkunden fehlt schlichtweg der notwendige Überblick über die durchgeführten Abbuchungen.

Da die Beanstandung[115] von berechneten Kosten nur möglich ist, wenn die reklamierten Beträge genau genannt werden, fehlt dem Prepaidkunden, der weder Gesamtrechnung noch Einzelverbindungsnachweis besitzt, jegliche Grundlage für eine Beanstandung. Der Mobilfunkkunde hat also per se über den Verbrauch seines Prepaidguthabens keinerlei Kontrolle und kann zudem auch nicht nachvollziehen, welcher Beteiligte welche Forderungen geltend macht. Ohne Überblick über berechtigte oder unberechtigte Forderungen von Drittanbietern ist es ihm somit im Zweifel unmöglich, sich gegen Drittanbieterforderungen zu wehren.

5.4 DIE REDIRECT-BEZAHLSEITE

Das bereits vorab erörterte Redirect-Verfahren stellt sich juristisch je nach Mobilfunknetzbetreiber und Drittanbieterangebot unterschiedlich dar. Allen Angeboten gemein ist, dass der Mobilfunkkunde zum Ende des Kaufprozesses von der Drittanbieterseite auf eine Bezahlseite weitergeleitet wird, die auf der technischen Plattform des Netzbetreibers liegt (siehe auch S. 30).

Auf dem Weg dorthin gelangen Telefónica-Kunden auf einer Seite des Drittanbieters oder des Aggregators, auf welcher der Vertragsschluss über die Leistung stattfinden soll. Diese Seite beinhaltet in der Regel Informationen über die Kündigungsmöglichkeit, den Preis sowie einen „Zahlungspflichtig bestellen“-Button.

112 Gem. § 45h TKG.

113 Siehe BT-Drs. 16/2581, Hoeren et al. (2016), Teil 4 - Telekommunikationsrechtliche Vorfragen Rn. 137.

114 Nach § 45e TKG.

115 Nach § 45i TKG.

Bei Kunden der Telekom und Vodafone ist dies nicht einheitlich geregelt. So ist zu beobachten, dass Verbraucher zunächst auf eine Drittanbieter- oder Aggregatorseite weitergeleitet werden, welche Informationen über die Kündigungsmöglichkeit, den Preis sowie einen „Weiter"-Button beinhalten. Auf dieser Seite soll offensichtlich noch kein Vertragsschluss stattfinden. Bei einigen Drittanbieterangeboten gelangt der Nutzer aber ohne vorherige Informationsseite direkt via Redirect auf die Bezahlseite und ist in manchen Fällen noch nicht darüber informiert, dass es sich bei dem Angebot um einen kostenpflichtigen Dienst handelt.

Sowohl bei der Telekom als auch bei Vodafone wird der eigentliche Vertragsabschluss erst auf dieser Bezahlseite mit einem Klick auf den „Zahlungspflichtig bestellen"-Button durchgeführt. Eine Besonderheit der Vodafone-Lösung ist, dass der Vorgang auf dieser Seite zusätzlich in zwei Schritte unterteilt ist: In einem ersten Schritt wird die Bezahlseite angezeigt (siehe S. 30), klickt man dort auf den Button „weiter", verändert sich die Beschriftung dieses Buttons auf „Zahlungspflichtig bestellen". Erst nach Betätigen dieses Buttons wird der Bezahlvorgang autorisiert.

Da die über das Redirect-Verfahren angesteuerte Bezahlseite vom Mobilfunknetzbetreiber betrieben wird, kann man davon ausgehen, dass dieser folglich auch entscheiden kann, nur am Markt rechtlich nicht zu beanstandende Drittanbieter für den Kaufprozess zuzulassen. Hier bietet sich ein Anknüpfpunkt an die bereits erwähnte Prüf- und Überwachungspflicht des Anbieters.

Insgesamt fällt bei allen getesteten Verfahren auf, dass weder auf der Seite des Mehrwertdiensteanbieters, noch auf der Bezahlseite der Mobilfunknetzbetreiber über das gesetzlich vorgeschriebene Widerrufsrecht aufgeklärt wird.

5.5 ZUSAMMENFASSUNG DER RECHTLICHEN ANALYSE

Räumt sich das Mobilfunkunternehmen das Recht ein, auch Drittanbieterforderungen vom Konto des Mobilfunkkunden einzuziehen, gebieten ihm unseres Erachtens Prüf- und Überwachungspflichten im Hinblick auf Rechte, Rechtsgüter und Interessen des Kunden. Davon umfasst sein können die Überprüfung der Einhaltung der Buttonlösung oder die Belehrung des Mobilfunkkunden über seine Widerrufsrechte. Eine Verletzung dieser Prüf- und Überwachungspflichten kann Schadensersatzansprüche aus allgemeinen Vorschriften gem. §§ 280 Abs. 1, 282, 249 ff. BGB zur Folge haben. Eine Möglichkeit, um dem Mobilfunkkunden frühzeitig und vor jeglichem Schaden die volle Kostenkontrolle zu bieten, wäre eine voreingestellte Drittanbietersperre, die ihm von Vertragsbeginn an ermöglicht, selbst zu entscheiden, wer auf sein mobiles Endgerät zugreifen darf und wer nicht. Dieser Ansatz würde sich vor allem für Prepaidkunden auszahlen, da diese bislang keinen Anspruch auf einen Einzelverbindungsnachweis nach § 45e TKG oder eine Gesamtrechnung haben, die zur Kostenkontrolle zwingend erforderlich sind. Dem Prepaidkunden bleibt damit nur der Weg der Beanstandung über den § 45i TKG, nachdem der Teilnehmer konkrete, schlüssige Gründe dafür angeben muss, dass die Abrechnung seines Erachtens nicht korrekt ist. Mit dem Redirect-Verfahren wurde bereits eine Maßnahme gegen unseriöse Drittanbieterforderungen ergriffen. Auffällig ist allerdings, dass im Rahmen dieses Verfahrens – sowohl auf der Webseite des Drittanbieters als auch auf der Redirect-Bezahlseite – häufig nicht ausreichend auf das gesetzlich vorgeschriebene Widerrufsrecht des Verbrauchers eingegangen wird.

6. MISSBRAUCHSSZENARIEN UND REDIRECT – UNTERSUCHUNG FRAUNHOFER INSTITUT

Wie stellen sich nun die Redirect-Verfahren der einzelnen Netzbetreiber in Bezug auf die genannten technischen Missbrauchsszenarien dar? Um deren Leistungsfähigkeit zu überprüfen, hat das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC im Auftrag des Marktwächters Digitale Welt, Schwerpunkt Telekommunikationsdienstleistungen, Ende 2016 ein Kurzgutachten erstellt.[116] Im Juli 2017 sind die eingesetzten Techniken erneut überprüft und Veränderungen dokumentiert worden.[117]

6.1 MISSBRAUCHSSZENARIEN MITTELS WEBBROWSER

In einem ersten Schritt wurden die Redirect-Bezahlseiten auf die Missbrauchsoption in einem Webbrowser hin untersucht, wie diese in Kapitel 2.3 beschrieben wurde. Dabei stellte sich die Frage: Können die Bezahlseiten der Netzbetreiber in eine schadhafte Internetseite geladen werden, sodass anschließend ein automatisierter, vom Verbraucher unbeabsichtigter Kauf über das Redirect-Verfahren herbeigeführt werden kann? Dazu wurden verschiedene, in diesem Zusammenhang relevante, Sicherheitskonzepte überprüft, die sich auf die Browser-App eines Smartphones beziehen: Die Same-Origin-Policy, das Framebusting, CSRF-Tokens und CAPTCHAS. Dabei ist der Einsatz eines Konzeptes allein für die moderne Sicherheitsarchitektur einer Web-Anwendung in der Regel nicht ausreichend. Diese Konzepte werden im Folgenden kurz erläutert.

6.1.1 Sicherheitskonzepte

Same-Origin-Policy

Diese Richtlinie regelt die Interaktion von Dokumenten oder Skripten, die von unterschiedlichen Internetadressen stammen. Über diese Regeln kann beispielsweise das Laden von Inhalten in ein kleines Webseiten-Fenster (iframe) sowie die Manipulation der geladenen Inhalte mittels Skriptcode eingeschränkt werden. Zusätzlich werden damit weit verbreitete Techniken gesteuert, welche die Benutzerfreundlichkeit von Webseiten deutlich erhöhen.[118] Allerdings kann diese Richtlinie aufgrund

METHODIK ZUR ÜBERPRÜFUNG REALISIERTER SCHUTZMASSNAHMEN

Ziel des Kurzgutachtens war die Untersuchung der zum Erstellungszeitpunkt eingesetzten Redirect-Lösungen der Mobile Network Operator Telefónica, Telekom und Vodafone vor dem Hintergrund eines wirtschaftlich motivierten Angriffs.

Testzeitraum
16. November – 15. Dezember 2016
Retest: Juli 2017

Technische Testspezifikationen
Android-Betriebssystem
Prepaid-SIM-Karten der entsprechenden MNO
Tests einer Click-Jacking-Protection der Redirect-Bezahlseiten vor dem Hintergrund

- des ausschließlichen Einsatzes eines Browsers,
- des Einsatzes eines Browsers mit einer installierten Browser-Extension,
- des Einsatzes einer Malware-App.

Durchführendes Institut
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC, München

Eine finale Aussage zur Sicherheit der eingesetzten Redirect-Lösungen sowie Aussagen über weitere Angriffsvektoren können aus dem Kurzgutachten nicht abgeleitet werden. Weitere Verwundbarkeiten in den beteiligten Endpunkten, zum Beispiel Missbrauch aufgrund fehlerhaften Codes in den Webbrowsern selbst, sind nicht Bestandteil der Betrachtung.

116 Vierthaler (2016).
117 Vierthaler (2017).
118 Damit sind asynchrone XmlHttpRequests gemeint, die die Kommunikation zwischen dem Webbrowser des Benutzers und einem Server über zwischengeschaltete Techniken ermöglichen, ohne dass der Benutzer seine Interaktion mit der Webanwendung unterbrechen muss, zum

ihrer Anlage durch verschiedene Angriffsmethoden[119] umgangen werden, sodass deren alleiniger Einsatz keinen ausreichenden Schutz beispielsweise gegen Clickjacking bietet.[120]

Framebusting

Eine weitere Methode, um das Laden von Inhalten einer Internetadresse in eine andere Webseite zu verhindern, ist das sogenannte Framebusting. Dieses macht sich das im Aufbau von Internetseiten enthaltene Schichtenmodell zunutze. Über einen eingebetteten Skriptcode wird überprüft, auf welcher Schicht sich der zu ladende Inhalt befindet. Je nachdem, welches Resultat die Überprüfung liefert, wird eine vorher festgelegte Aktion angestoßen. Diese Methode ist jedoch auf aktivierten Skriptcode (Javascript) im Webbrowser angewiesen. Das ist Vor- und Nachteil zugleich: Der Vorteil liegt darin begründet, dass diese Methode auch mehrstufig implementiert werden kann, um einen effektiveren Schutz zu erzeugen.[121] Die einfachste Ausführung von Framebusting besteht aus einer Prüfung, ob der eingebettete Inhalt auf der obersten Schicht liegt. Wenn dies nicht der Fall ist, leitet das Skript automatisch auf die richtige Internetadresse weiter. Bei mehrstufigen Varianten wird der Inhalt der Webseite zunächst über definierte Formatierungsanweisungen verborgen. Danach folgt eine Prüfung, ob sich der Inhalt auf der obersten Schicht befindet. Sofern das Ergebnis positiv ist, werden die Formatierungsanweisungen wieder entfernt und der Inhalt wird sichtbar. Ist das Resultat hingegen negativ, so wird, analog zur einfachen Variante, auf die korrekte Internetadresse weitergeleitet.

Wenn die Ausführung von Skriptcode im Webbrowser deaktiviert ist, wirken die dargestellten Methoden nicht in der vorgesehenen Weise. Insbesondere bei der Missbrauchsoption des Clickjackings im Zusammenhang mit einem iframe spielt das eine wichtige Rolle. Über sogenannte Sandbox-Parameter des iframes kann gesteuert werden, ob in der eingebetteten Seite Skriptcode ausgeführt werden darf und somit überhaupt auf die korrekte Seite weitergeleitet werden kann. In diesem Fall böte die einfache Variante keinen Schutz gegen Missbrauch.

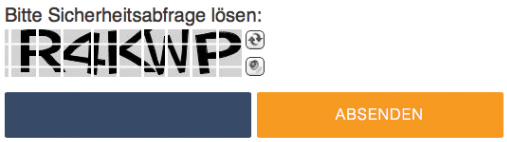
CSRF-Token

Im Oktober 2016 hatte der Chaos Computer Club Hannover im neuen WLAN der ICEs eine Schwachstelle offenbart. Dabei können gültige Sitzungsdaten zwischen einem anzugreifenden Server und dem Browser eines Opfers ausgenutzt werden, um schädliche Anfragen zu versenden.[122] Diese Schwachstelle beziehungsweise die damit einhergehende Angriffsoption wird Cross-Site-Request-Forgery (CSRF) genannt. Um Angriffe dieser Art abzuwehren, können Identifikationsmerkmale eingesetzt werden, sogenannte CSRF-Tokens, die bei jedem Webseitenaufruf neu und zufällig generiert werden. Diese Tokens werden auf dem Server abgelegt und derart in die Webseiten eingebettet, dass sie bei jeder Anfrage mitgeschickt werden. Bei einer späteren Bearbeitung durch den Server kann dieser dann anhand verschiedener Kriterien überprüfen, ob das gelieferte Identifikationsmerkmal gültig ist und die gewünschte Aktion ausführen.[123]

CAPTCHA

Häufig nutzen Kriminelle kleine Programme, um automatisiert Formulare auf Webseiten zu versenden. Sogenannte CAPTCHAs[124] helfen Webanwendungen, den Zugriff zwischen Mensch und Maschine auf eine Aktionsfläche zu unterschieden. Nachfolgend ist der beispielhafte Einsatz eines CAPTCHAs dargestellt:

18 BEISPIELHAFTE DARSTELLUNG EINES CAPTCHAS



Quelle: https://www.denic.de/webwhois/

Der Nutzer der Webseite muss den Inhalt des dargestellten Bildes, in diesem Fall R4KWP, in das blaue Feld eintragen und anschließend auf „Absenden“ drücken. Nur wenn der eingetragene Inhalt mit dem dargestellten Inhalt übereinstimmt, wird die Aktion, zum Beispiel

Beispiel weil eine neue Seite geladen werden muss oder eine Sanduhr angezeigt wird. Garrett (2005).

119 Z. B. Man-in-the-middle Angriff oder über ein Browser Addon.

120 Vgl. Vierthaler (2016), S. 2 ff.

121 Vgl. ebda., S. 4 ff.

122 Siehe Chaos Computer Club Hannover e. V. (2016). Diese Schwachstelle besteht im Juli 2017 nach wie vor, siehe Chaos Computer Club Hannover e. V. (2017).

123 Vgl. Vierthaler (2016), S. 6.

124 Completely Automated Public Turing test to tell Computers and Humans Apart.

das Absenden eines Formulars, ausgeführt. In der Praxis stellen CAPTCHAs häufig einen wirksamen Schutz vor leichter Automatisierung dar; jedoch können CAPTCHAs beispielsweise mithilfe eines Online-Captcha-Services (z. B: https://anti-captcha.com/) auch im Rahmen eines automatisierten Skripts gelöst werden, sodass sie keinen alleinigen Schutz darstellen.

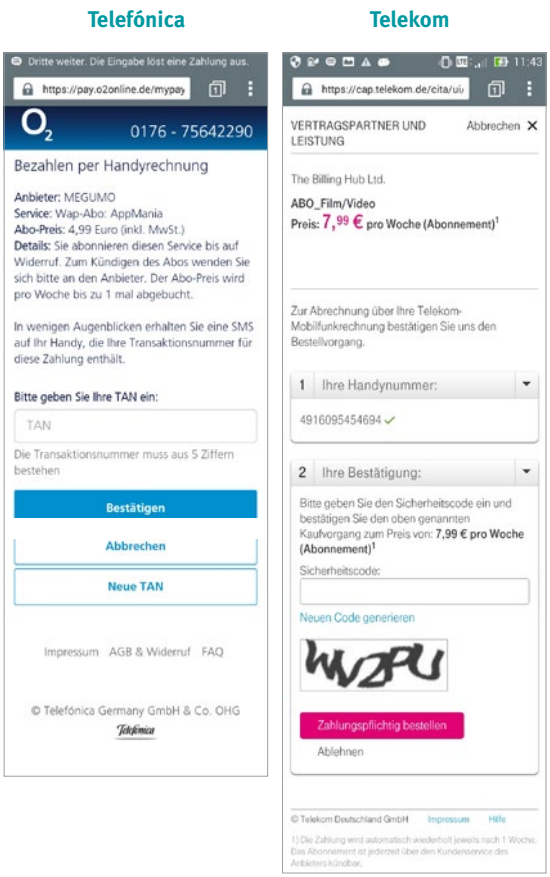
6.1.2 Beobachtungen bei den einzelnen Mobilfunknetzbetreibern

Bei dem Netzbetreiber **Telefónica** ist zwischen dem ersten und zweiten Testzeitraum eine deutliche Veränderung zu beobachten. Während Ende 2016 die Bezahlseite, auf die das Redirect-Verfahren weiterleitete, noch implementiert war, ist diese im Juli 2017 bei den getesteten Drittanbieterangeboten durch eine Seite ausgetauscht worden, in die durch den Nutzer eine TAN für den Abschluss des Abonnements eingegeben werden muss. Bis auf das TAN-Verfahren unterscheiden sich die Schutzmechanismen dieser unterschiedlichen Bezahlseiten jedoch nicht.[125] **Telefónica** setzt mehrere Techniken ein, um das Laden dieser Bezahlseite in andere Webseiten zu unterbinden. Dabei werden unterschiedliche Aspekte der Same-Origin-Policy genutzt und mit entsprechenden Werten versehen. Weiter wird ein mehrstufiger Framebusting-Mechanismus eingesetzt, der ein Clickjacking über den Webbrowser wirkungsvoll verhindert. Ein CSRF-Schutz ist durch den Einsatz entsprechender Identifikationsmerkmale gegeben. Wird dieses Merkmal modifiziert, so wird der Bestellvorgang vom Server als ungültig erkannt und schlägt fehl.[126]

Die **Deutsche Telekom** setzt auf einen mehrstufigen Framebusting-Prozess, mit dem das Clickjacking verhindert wird. Auch bei der Telekom ist ein CSRF-Schutz gegeben, der durch einen Token sichergestellt wird. Dieser wird auf dem Telekom-Server generiert und bei einer Bestellung zur Prüfung an eben diesen Server gesendet. Ist der Token ungültig, schlägt die Bestellung fehl.[127]

Vodafone setzt Elemente der Same-Origin-Policy ein, um das Laden der Redirect-Bezahlseite in eine andere Webseite zu verhindern. Auch eine im Hintergrund laufende Kommunikation zwischen Nutzer und Server[128] wird unterbunden. Eine Bewertung der CSRF-Sicherheit ist hingegen nicht möglich. Zu beiden Untersuchungszeitpunkten existiert keine Aussage darüber, ob Drittanbieter oder Aggregator während der Weiterleitung auf die Redirect-Anwendung Zugriff auf einen bestimmten Sitzungsparameter besitzen oder nicht. Ist sichergestellt, dass ein Angreifer keine Kenntnis über diesen Parameter erlangen kann, so ist ein Angriff aus dieser Richtung unwahrscheinlich, sofern diese Parameter zufällig erzeugt werden. Falls der Parameter abgreifbar ist, wäre eine CSRF-Attacke möglich, da während der Untersuchung kein Schutz vor Automatismen bestand und ein Token zwar in der Webseite eingebettet war, serverseitig aber nicht geprüft wurde.[129]

19 REDIRECT-BEZAHLSEITEN MIT SICHERUNGSMECHANISMEN



Quelle: Telefónica Germany GmbH & Co. OHG (Stand: Juli 2017), Telekom Deutschland GmbH (Stand: Juli 2017)

125 Vgl. Vierthaler (2017), S. 10 ff.
126 Vgl. Vierthaler (2016), S. 12 ff.
127 Vgl. ebda., S. 10 ff.
128 Via XmlHttpRequest.
129 Vgl. Vierthaler (2016), S. 7 ff.

Im Rahmen des Kurzgutachtens konnte Ende 2016 durch das Fraunhofer-Institut bei keinem Netzbetreiber Schutz vor automatisierten Anfragen, zum Beispiel in Form von CAPTCHAs, bei den getesteten Angeboten festgestellt werden. Im Juli 2017 wird nun im Telekom-Redirect-Verfahren bei jedem Aufruf der getesteten Webseiten ein CAPTCHA abgefragt. Dieses Vorgehen bietet somit einen Schutz beispielsweise vor einfachen Angriffen über eine Smartphone-App, die mittels schadhaftem Code eine Webview steuert.[130]

6.1.3 Besonderheit: Webextensions

Der Nachteil der auf der Same-Origin-Policy basierten Schutzmechanismen besteht darin, dass sie durch eine Manipulation in den Einstellungen des eigenen Browsers ausgehebelt werden können. Dies könnte beispielsweise auch über eine sogenannte Webextension erreicht werden. Webextensions sind kleine Zusatzprogramme, die den Funktionsumfang eines Browsers erweitern, beispielsweise als Blocker gegen Werbebanner. Diesen Erweiterungen ist es möglich, auf eine große Anzahl spezieller Browserfunktionen zuzugreifen und darüber unter anderem auch den Teil zu modifizieren, der für eine domänenübergreifende Kommunikation notwendig ist. Zudem können einzelne Anfragen blockiert und so Schutzmechanismen umgangen werden. Der Einsatz einer entsprechenden Erweiterung im Zusammenhang mit den Redirect-Verfahren der Netzbetreiber bescheinigt zumindest der Telekom und Telefónica einen ausreichenden Schutz vor Manipulation. Bei der Vodafone-Variante des Redirect-Verfahrens wäre es einem Angreifer jedoch möglich, mittels Webextension einen Clickjacking-Angriff erfolgreich durchzuführen.[131]

6.2 MISSBRAUCHSSZENARIEN MITTELS SMARTPHONE-APPLIKATION

Mit einer wachsenden Anzahl der Smartphone-Nutzer in Deutschland[132] steigt auch die Menge an App-Downloads[133]. Damit stellt auch der missbräuchliche Abschluss eines Drittanbieterabonnements über eine präparierte Smartphone-App ein denkbares Szenario dar, insbesondere da sich viele Nutzer nicht bewusst sind, welche Berechtigungen sie der einzelnen Applikation auf ihrem Smartphone geben.[134] Eine solche Anwendung bietet außerdem den Vorteil, dass sie sich direkt an die Zielgruppe der Mobilfunkkunden richtet und damit eine Abrechnung via Mobilfunkvertrag einfach möglich ist.

6.2.1 Aufbau und Funktion der Testapplikation

Um dieses Missbrauchsszenario zu testen, wurde Ende 2016 das Grundgerüst einer Smartphone-App entwickelt. Dieses verwendet eine sogenannte Webview[135], eine Komponente innerhalb des jeweiligen „Programmiergerüstes“, auf welchem Apps aufbauen. Diese ermöglicht die Darstellung und Interaktion mit Webseiten innerhalb der installierten Smartphone-App. Unter anderem kann darüber auch beliebiger Skriptcode (Javascript) in eine geladene Webseite eingeschleust werden. Ziel dieser Testanwendung ist es, Aktionen auf den Drittanbieterseiten durchzuführen und von dort aus auf die Redirect-Bezahlseiten der Netzbetreiber weiterzuleiten, um anschließend ein Abonnement abzuschließen, ohne dass der Anwender Einfluss darauf nehmen kann.

In einem Testszenario lädt die Applikation zunächst die Seite eines Drittanbieters. Dort interagiert sie mit den relevanten Komponenten, um den Redirect einzuleiten. Ist die Adresse der Redirect-Anwendung geladen, so wird ein Skript eingeschleust, welches den jeweiligen Button aktiviert. Damit kann erfolgreich ein Abonnement über die Redirect-Bezahlseite abgeschlossen werden. Sofern notwendig, kann der Angreifer die Vorgänge mit einem weiteren Skriptcode verschleiern, sodass der Benutzer auch optisch keinen Hinweis auf die durchgeführte Aktion erhält. Fehlende Sicherheitsmechanismen auf den Redirect-Bezahlseiten gegenüber automatisierten Zugriffen erhöhen die Zuverlässigkeit für den Abschluss eines Abonnements.

6.2.2 Beobachtungen bei den einzelnen MNO/Mobilfunknetzbetreibern

Vor dem Hintergrund des dargestellten Testszenarios ist die Telekom-Redirect-Lösung im Juli 2017 gegen einfache, automatisierte Angriffe im Vergleich zu den Lösungen der anderen Netzbetreiber durch die Verwendung von CAPTCHAS zumindest besser geschützt.

130 Vgl. Vierthaler (2017), S. 5 ff.
131 Vgl. Vierthaler (2016), S. 15 ff.
132 Vgl. comScore (2016).
133 Vgl. Bitkom e.V. (2014).
134 Siehe Felt et al. (2012) und Wijesekera (2015).
135 Siehe zum Beispiel Google (o. J.) und Apple (2016) oder zusammengefasst bei Looper (2015).

Das TAN-Verfahren von Telefónica besitzt hingegen nur einen eingeschränkten Schutz gegen eine schadhafte App, wenn diese sowohl Berechtigungen für den Internet-Zugriff als auch Zugriff auf die SMS des Benutzers besitzt. Für einen entsprechenden Angriff würde die schadhafte Applikation mittels einer modifizierten Webview selbstständig auf die TAN-Seite von Telefónica weiterleiten. Anschließend könnte die Applikation die eingehende SMS auslesen und diese automatisiert in das TAN-Feld der Anwendung einfügen.

Da die Vodafone-Lösung weder CAPCTHAS noch ein TAN-Verfahren einsetzt, ist sie von den hier untersuchten Varianten nicht gegen mögliche Automatismen geschützt und bietet somit den geringsten Schutz.[136]

6.3 ZUSAMMENFASSUNG DER ÜBERPRÜFUNG VON MISSBRAUCHSSZENARIEN UND REDIRECT-VERFAHREN

Die durchgeführten Prüfungen zeigen, dass der für einen Angreifer kosteneffizienteste Weg, unabsichtliche Drittanbieterabos über den Webbrowser zu initiieren, nicht mehr zur Verfügung steht. Das Redirect-Verfahren der Netzbetreiber bietet nach aktuellem Kenntnisstand gegen die hier untersuchte Angriffsmethode über **einen Webbrowser** einen ausreichenden Schutz.

Ein Angriff mittels **Webextensions** würde es dem Angreifer zwar ermöglichen, den Vodafone-Redirect im Rahmen einer Clickjacking-Attacke zu verwenden, diese Webextension müsste jedoch erst über die notwendigen Wege (Browser-Store) verbreitet werden. Die Prüfung der Browsererweiterungen durch den Store-Betreiber sowie die Notwendigkeit, einen Vodafone-Kunden zu bewegen, diese Erweiterung auf seinem internetfähigen Gerät zu platzieren, reduziert die Wahrscheinlichkeit eines erfolgreichen technischen Missbrauchs.[137]

Die Möglichkeit, über eine **schadhafte Smartphone-Applikation** einen strittigen Vertragsschluss herbeizuführen, erscheint aus Sicht der Angreifer von den hier betrachteten Ansätzen derzeit wirtschaftlich als am erfolgversprechendsten. Der Vertrieb einer solchen App, zum Beispiel über den Google Play Store, ist vergleichsweise einfach und wendet sich unmittelbar an Mobilfunkteilnehmer als Adressaten. Da der Angriffscode in der App lediglich Zugriff auf das Internet und bei Telefónica zusätzlich auf die SMS-Funktionalität benötigt, kann er auch unbemerkt in legitime Smartphone-Anwendungen integriert werden. Das kann in Form einer Programmbibliothek (Library) geschehen, die – gegebenenfalls auch in Unwissenheit ihrer Funktionalität – durch den App-Entwickler eingebunden wird. Des Weiteren können auch Angriffe auf das sogenannte „Dynamic Class Loading“ unter Android realisiert werden, indem Skriptcodes in laufende Apps injiziert werden.

Auch eine triviale Verbreitung als eigene App durch den Missbrauchsurheber oder einen Mittelsmann über den App-Store ist vorstellbar, da die dortigen Prüfmechanismen erfahrungsgemäß die hier beschriebenen Angriffsvektoren nicht abdecken.[138] [139] Inwiefern das in 2017 eingeführte Google Play Protect Nutzer vor Apps mit enthaltendem Angriffscode schützt, bleibt abzuwarten.

Außerdem wäre die Streuung einer derartigen App als Download über unsichere Stores denkbar, müsste aber wohl durch entsprechende Anreize unterstützt werden, zum Beispiel in Form einer von Seiten der Verbraucher wünschenswerten Besonderheit.[140]

Festzuhalten bleibt, dass Verbraucher durch das eingeführte Redirect-Verfahren der Netzbetreiber gegen Clickjacking über den Browser eines Smartphones geschützt sind. Durch den Einsatz einer Webextension im Browser kann hingegen das Redirect-Verfahren von Vodafone umgangen werden. Im Zusammenhang mit einer schädlichen Applikation auf dem Smartphone bietet das Redirect-Verfahren als alleinige Sicherheitskomponente keinen Schutz. Der Einsatz von CAPTCHAS kann in diesem Fall das Risiko des Missbrauchs reduzieren – aber nicht restlos ausschließen. Im Vergleich steht somit die Lösung der Telekom derzeit am besten dar.[141]

136 Vgl. Vierthaler (2017), S. 10 und S. 14.
137 Vgl. Vierthaler (2016), S. 17 ff.
138 Vgl. Vierthaler (2016), S. 18 ff.
139 Siehe auch Bartsch et al. (2014), Stefanko (2015), Whitwam (2012).
140 Vgl. Weidner (2016).
141 Vgl. Vierthaler (2017), S. 14.

7. FAZIT UND SCHLUSSFOLGERUNGEN

Bei dem hier untersuchten Problem der strittigen Drittanbieterposten, die auf einer Mobilfunkrechnung auftauchen, handelt es sich um ein komplexes Thema mit vielen Facetten. Der Bericht konzentriert sich auf die Klärung der Gründe für den Anstieg von Beratungen zu dieser Problematik in den Verbraucherzentralen bis in den Untersuchungszeitraum hinein, sowohl in technischer als auch in rechtlicher Hinsicht. Zudem werden die Ausprägungen für die Betroffenen analysiert und deren Verbreitung in der Bevölkerung untersucht. Die anbieterseitig eingeführten Sicherungsmechanismen zum Schutz der Verbraucher werden differenziert betrachtet und das Redirect-Verfahren im speziellen einem technischen Test unterzogen. Darüber hinaus gibt es aber noch weitere Aspekte, die nicht oder nicht in aller Tiefe diskutiert werden konnten, so wie beispielsweise der Jugendschutz oder das Haftungsproblem von Drittanbietern, die nicht in Deutschland angesiedelt sind.

Mobiles Bezahlverfahren mit viel Potential

Das betrachtete WAP-Billing beziehungsweise Direct Billing ist als Bezahlverfahren dem Carrier Billing als übergeordnetem Geschäftsmodell zuzurechnen. Als inkassobasiertes System setzt das Carrier Billing aus Perspektive des Verbrauchers auf der bestehenden Vertragsbeziehung zum Telekommunikationsanbieter auf, dessen Rechnungen dann Drittanbieterleistungen beinhalten können.

Transaktionen über dieses Bezahlverfahren werden in der Regel über eine mobile Internetsitzung aus räumlicher Entfernung durchgeführt. Vereinfacht ausgedrückt erfolgt ein Vertragsschluss beim Direct Billing, indem der Verbraucher über die Browser-Applikation seines Smartphones die Webseite eines Drittanbieters öffnet und dort via Klick auf einen Button die Leistung bestellt, ohne sich zusätzlich einloggen oder ein Bezahlverfahren auswählen zu müssen. Die Identifizierung des Nutzers erfolgt über die durch den Netzbetreiber weitergeleitete Mobilfunknummer (MSISDN) oder ein vergleichbares Kriterium, um die Leistung berechnen zu können.

Mit sechs Prozent lag der Bezahlweg über die Telefonrechnung im Jahr 2015 laut einer Studie des Bundesverband E-Commerce und Versandhandel Deutschland e. V. deutlich hinter anderen Optionen zurück, beispielsweise der Kreditkarte mit 41 Prozent oder dem Bankeinzug mit 27 Prozent.[142] Mit prognostizierten Umsätzen von knapp 14 Milliarden Euro im Markt der digitalen Inhalte in Europa für das Jahr 2020 bietet sich für die Marktakteure jedoch ein großes Potential für das Carrier Billing im Allgemeinen, insbesondere dann, wenn die erweiterten Möglichkeiten, digitale Inhalte zu nutzen, in die Betrachtung einbezogen werden, beispielsweise über den Smart TV oder innerhalb des vernetzten Automobils.[143] Damit ist dieser Markt und das hier besprochene Bezahlverfahren eben auch weiterhin für kriminelle Akteure interessant.

Die Drittanbieterproblematik als Dauerthema in den Verbraucherzentralen

Neu sind die Ärgernisse mit sogenannten Drittanbietern, also mit den Anbietern der in Rechnung gestellten Leistungen, nicht. Bereits seit der Zeit von Klingelton-Abos in den frühen 2000er Jahren[144] beschäftigt dieses Thema die Verbraucherzentralen in Deutschland. Mit der Novellierung des Telekommunikationsgesetzes (TKG) im Jahr 2012[145] wurden zwar verbraucherfreundlichere Regelungen festgelegt, beispielsweise die kostenfreie Einrichtung einer Drittanbietersperre auf Wunsch des Verbrauchers[146], strittige Sachverhalte, die sich durch den Abschluss von Rechtsgeschäften über WAP-Schnittstellen ergaben, blieben aber weiterhin ungelöst.

Im Zusammenhang mit dem zugrundeliegenden Sachverhalt zeigt die qualitative Analyse des FWN in einem ersten Schritt, dass Verbraucher dann Hilfe in den Beratungsstellen der Verbraucherzentralen suchen, wenn sie unbeabsichtigt Leistungen Dritter ausgelöst haben oder den Abschluss nicht nachvollziehen können. Dabei ist zu beobachten, dass die Kenntnisnahme über den Vertragsschluss nicht immer unmittelbar erfolgte, sondern erst zu einem späteren Zeitpunkt, zum Beispiel bei der Prüfung der Mobilfunkrechnung. Aufgrund der Unkennt-

142 Siehe Interaktiver Handel in Deutschland, Ergebnisse 2015, Bundesverband E-Commerce und Versandhandel e. V. (2016), S. 30.
143 Vgl. Juniper Research/Dimoco (2016), S. 16 ff.
144 Siehe z. B. vzbv (2003), S. 10 ff.
145 Deutscher Bundestag (2015).
146 Deutscher Bundestag (2011), S. 21.

nis über einen Vertragsschluss interpretieren manche Verbraucher erhaltene Bestätigungs-SMS über ein Abonnement beispielsweise auch als Spam und können deren Auswirkungen nicht richtig einschätzen.

Die Vertragspartner der Verbraucher zeigen sich durchaus entgegenkommend, zum Beispiel durch Rückerstattung und Einrichtung einer Drittanbietersperre. Andererseits sind in der Beratung der Verbraucherzentralen auch Fälle zu beobachten, in denen Anbieter auf ihren Forderungen beharren und zur Durchsetzung zum Beispiel mit einer Rufnummernsperre drohen und diese auch teilweise durchführen.

Die Einzelkosten pro Abo liegen in der Regel unter 10,00 Euro pro Woche, die Gesamtkosten des entstandenen Schadens können hingegen deutlich höher ausfallen. Dabei kommt es in vielen Fällen auf den Zeitpunkt an, zu dem den Verbrauchern das Abonnement auffiel. In Einzelfällen kann der Schaden bei bis zu mehreren Tausend Euro liegen.

Weite Verbreitung und hoher Schaden

Die Erfahrungen aus den Verbraucherzentralen werden weitestgehend durch die bevölkerungsrepräsentative Umfrage gestützt. Grundlegend wird jedoch deutlich, dass das Bezahlen von Leistungen Dritter über die Mobilfunkrechnung bisher nur von wenigen Verbrauchern genutzt wird (8 Prozent im Zeitraum von 2013 bis 2016). Nur ein Drittel der befragten Verbraucher, denen bereits Leistungen Dritter von ihrem Mobilfunkvertrag abgebucht wurden, gaben an, dass es sich dabei um absichtlich abgeschlossene Posten handelte. Der Markt scheint demnach mehrheitlich von Missbrauch durchzogen zu sein. Hochgerechnet auf alle deutschsprachigen Mobilfunknutzer ab 14 Jahren bedeutet dies, dass schätzungsweise 2,2 bis 3,4 Millionen Personen in Deutschland innerhalb der letzten 3 Jahre betroffen waren.[147]

Gefragt nach der Höhe der Gesamtkosten durch einen unabsichtlichen Abonnementschluss ergibt sich ein ähnliches Bild wie in den Sachverhalten aus dem FWN. Die Befragten gaben Kosten in Höhe von 1,00 Euro bis 1.000 Euro in einem Jahr an. Die durch den unabsichtlichen Abschluss von Drittanbieterleistungen entstandenen durchschnittlichen Gesamtkosten betrugen 86,52 Euro (Median: 25,52 Euro; Modus: 5,00 Euro). Die zum Teil hohen Kosten können dabei auf die Tatsache zurückzuführen sein, dass unabsichtliche Abschlüsse nicht immer sofort wahrgenommen und auch die Rechnungen nicht regelmäßig eingesehen werden. So prüfen 17 Prozent der Befragten ihre Rechnung nie oder nicht persönlich, meist weil sie ihrem Anbieter vertrauen (23 Prozent) oder weil diese Aufgabe von jemand anderem aus ihrem Umfeld wahrgenommen wird (21 Prozent).

Werden die vorangegangenen Zahlen zu Geschädigten und durchschnittlichen Gesamtkosten durch einen unabsichtlichen Abonnementabschluss zugrunde gelegt, so sind nach eigenen Berechnungen den Mobilfunknutzern ab 14 Jahren in Deutschland im Zeitraum von 2013 bis 2016 Gesamtkosten in Höhe von ca. 71,5 Millionen Euro (Schätzintervall ± 15,31 Millionen Euro) entstanden.[148]

Unzureichende Prüfverfahren

Ein Bezahlverfahren wie es hier beschrieben ist, wird nur verwendet, wenn es einen Zusatznutzen bietet, verbraucherfreundlich ist und auch Vertrauen in dieses Verfahren besteht.[149]

Schon seit vielen Jahren wird jedoch mit einer gewissen Regelmäßigkeit in den Medien über Missbrauchsfälle im Zusammenhang vor allem mit dem WAP-Billing oder Direct Billing berichtet,[150] die dieses Bezahlverfahren mit einem Vertrauensverlust belasten. Deshalb gibt es auch auf der Anbieterseite Bemühungen, den Telekommunikationsmarkt vom Drittanbieterproblem zu befreien. Mit der Clean-Market-Initiative, einer gemeinsamen Qualitätsoffensive deutscher Mobilfunknetzbetreiber, haben die Mitglieder seit 2012 ein Freischaltungs- und Testverfahren aufgebaut, das Anbieter und deren Leistungen zu Beginn des Betriebes formal und qualitativ überprüft.[151] Erst nach bestandener Prüfung können deren Leistungen über die Mobilfunkrechnung abgewickelt werden. Die Resultate der Umfrage und auch die vorliegenden Fälle im FWN belegen allerdings, dass diese Kontrolle nicht immer gut funktioniert. Dabei stellt sich die Frage, ob dies in der notwendigen Form und der Anzahl an Drittanbieterangeboten überhaupt möglich ist. Allein

147 Abschluss Umfrage: August 2016.

148 Siehe Kapitel 3.2.

149 Siehe z. B. Scholz (2016) und vgl. Klees et al. (2013).

150 Vgl. z. B. Bleich (2011), Zeit Online (2015) oder mdr (2016).

151 Siehe Kapitel 4.2.

die Prüfung formaler Kriterien wie zum Beispiel Adressdaten, Handelsregistereintrag und verantwortliche Personen helfen durch die unterschiedlichen rechtlichen Ansätze innerhalb der EU nur teilweise. Auch qualitative Kriterien wie die Nachhaltigkeit und das Leistungsversprechen des Angebotes scheinen für eine Bewertung der Seriosität des Angebotes in diesem Zusammenhang kein ausreichend sicherer Maßstab zu sein. Die von der mdk GmbH im Auftrag der Netzbetreiber durchgeführten 250 Stichproben pro Monat in Bezug auf die Drittanbieterwebseiten sind vor dem Hintergrund der erhobenen Daten als zu gering einzustufen.

Schwachstellen aus rechtlicher Perspektive

In puncto Verbraucherfreundlichkeit wird deutlich, dass Mobilfunkkunden mit Prepaidverträgen im Vergleich zu denen mit Postpaid-Verträgen in Bezug auf die Drittanbieterproblematik schlechter geschützt sind, da in diesem Bereich normalerweise keine Rechnungstellung erfolgt. Der Prepaidkunde hat keinen Anspruch auf Erteilung eines Einzelverbindungsnachweises. Ohne diesen kann er Rechnungspositionen nicht schlüssig und substantiiert beanstanden.

Außerdem muss die Zulässigkeit von den derzeit verwendeten pauschalen Inkassoklauseln[152] als vorformulierte Geschäftsbedingung im Prepaidbereich[153] hinterfragt werden, da über das Prepaidguthaben Beträge eingezogen und abgeführt werden, bezüglich derer der Verbraucher aufgrund der fehlenden Information keinen Überblick hat und sich deshalb nicht zur Wehr setzen kann.

Unabhängig davon, ob es sich um einen Post- oder Prepaidvertrag handelt, steht bei dieser Thematik zur Diskussion, ob die Inkassoklauseln für die Anwendung im Bereich der Verbrauchergeschäfte zu unbestimmt sind. Zum Zeitpunkt der Vereinbarung der AGB sind weder Drittanbieter noch Höhe der Zahlung noch Laufzeit des Inkassos bekannt. Es bieten sich alternative Zahlungsmethoden, die sich auf ein konkret bestimmtes Vertragsverhältnis beziehen und schon deswegen verbraucherfreundlicher sind.

Wenn sich aber das Mobilfunkunternehmen über diese Inkassoregeln das Recht einräumt, auch Drittanbieterforderungen vom Konto des Mobilfunkkunden einzuziehen, ergeben sich daraus im Rückschluss auch Prüf- und Überwachungspflichten im Hinblick auf Rechte, Rechtsgüter und Interessen des Kunden. Die Ausgestaltung dieser Pflichten sollte sich zumindest in der Überprüfung der Einhaltung der Buttonlösung oder die Belehrung des Mobilfunkkunden über seine Widerrufsrechte äußern. Eine Verletzung dieser Prüf- und Überwachungspflichten kann dann allgemeine Schadensersatzansprüche nach sich ziehen.

Mit dem Redirect-Verfahren als anbietergestützte Maßnahme gegen unerwünschte Drittanbieterabonnements ist nun eine neue Komponente in den technischen Ablauf eingebracht worden. Über dieses kann der Direct Billing-Bezahlprozess, das heißt das Einkaufen und Bezahlen über das mobile Internet, für eine Drittanbieterleistung auf der technischen Infrastruktur der Netzbetreiber abgeschlossen werden. Für den Verbraucher äußert sich der Redirect in einer Weiterleitung von der Webseite des Drittanbieters, auf der das Angebot präsentiert wird, hin zu einer Bezahlseite, die sich optisch eindeutig von der vorherigen Seite unterscheidet.[154]

Aus rechtlicher Perspektive stellt sich die Redirect-Bezahlseite dabei als unterschiedlich ausgestaltete Einmischung in den Vertrag über Mehrwertdienstleistungen dar. Im elektronischen Geschäftsverkehr ist eine vergleichbare Einmischung eines weiteren Akteurs während des Abschlusses eines Vertrages bisher nicht zu finden und deshalb zu diesem Zeitpunkt rechtlich nicht eindeutig einzuordnen. Zumindest ermöglicht diese Bezahlseite eine konsequentere Überprüfung der Kaufvorgänge im Vergleich zu der Zeit vor Einführung des Redirect-Verfahrens, da der Abschluss nun auf der Infrastruktur der Netzbetreiber stattfindet. Damit wird beispielsweise einfacher Betrug durch die Meldung falscher Daten an die Netzbetreiber ausgeschlossen, sodass der Verbraucherschutz in Bezug auf die Abrechnung gestärkt wird. Unabhängig davon ist zu beobachten, dass der Einsatz des Redirect-Verfahrens nicht dazu geführt hat, dass im Rahmen dieses Prozesses die gesetzlich vorge-

152 Zum Beispiel: „3. Vergütung 3.1....Vodafone ist berechtigt, Entgelte für Verbindungen zu Diensteangeboten Dritter geltend zu machen, zu denen Vodafone die Verbindung herstellt." Vodafone GmbH (2016), abgerufen am 31.07.2017.

153 „6.5 Die vereinbarten Preise für Leistungen einschließlich sämtlicher Preise, zu denen congstar den Zugang vermittelt, werden von dem Guthaben des Kontos in Abzug gebracht. Ziffer 6.2 Satz 3 gilt entsprechend." Congstar (2016), abgerufen am 31.07.2017.

154 Siehe Kapitel 4.3.

schriebenen Informationspflichten eingehalten werden und unter anderem ordnungsgemäß auf das gesetzlich vorgeschriebene Widerrufsrecht des Verbrauchers hingewiesen wird.

Durch die seit dem 04.07.2017 geltende Vorschrift § 45d Abs.4 TKG[155], wonach die Bundesnetzagentur Verfahren festzulegen hat, die den Mobilfunknutzer wirksam davor schützen, „dass eine neben der Verbindung erbrachte Leistung gegen seinen Willen in Anspruch genommen und abgerechnet wird.“, könnte die künftige Ausgestaltung und Funktion der Redirect-Bezahlseite, insbesondere in Bezug auf die gesetzlich geregelten Informationspflichten wie die Darstellung der wesentlichen Eigenschaften der Waren oder Dienstleistungen, die Identität des Unternehmers, Gesamtpreis und ggf. Vertragslaufzeit, Hinweise zum Widerrufsrecht[156], eine neue Qualität geben. Eine einheitliche Ausgestaltung solch eines von der Bundesnetzagentur ausgestalteten Verfahrens hätte zur Folge, dass – entgegen der bisherigen Praxis – der Vertragsschluss einschließlich der erforderlichen Pflichtinformationen und unabhängig von dem eigentlichen Leistungsanbieter, eindeutig auf der Redirect-Bezahlseite der Mobilfunknetzbetreiber erfolgt. Durch die Abbildung dieser Informationen, ließe sich auch die zuvor aufgeworfene Frage der pauschalen Inkassovereinbarungen zwischen Mobilfunkkunden und MNO klären, da die Redirect-Bezahlseite somit auch eine ausreichende Konkretisierung darstellte.

Das Redirect-Verfahren aus technischer Sicht

Vor einem technischen Hintergrund ist die Einführung des Redirect-Verfahrens für den Verbraucher jedoch erst einmal von Vorteil. Denn damit ist nun zumindest eine Möglichkeit des technischen Missbrauchs mittels Webbrowser in einer mobilen Internetsitzung geschlossen worden. Eine technische Überprüfung des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC ergab, dass die Redirect-Bezahlseiten durch mehrstufige Sicherheitsmechanismen vor dem oben genannten Clickjacking-Angriff über die Nutzung eines Webbrowsers geschützt werden können.[157] Seit der Einführung des Redirect-Verfahrens ist laut Netzbetreibern ein deutlicher Rückgang der Kundenanfragen zu diesem Thema zu beobachten und auch die Bundesnetzagentur verweist auf sinkende Beschwerdezahlen.[158]

Für welche Angebote dieses Verfahren eingesetzt wird, obliegt bisher den Netzbetreibern, die sich vorbehalten, Angebote von dem Redirect-Verfahren auszuschließen. Für Einzelkäufe steht der Einsatz generell in Frage.[159]

Ein flächendeckender Einsatz dieses Verfahrens könnte aber helfen, Missbräuche weitgehend abzuwehren. Damit wäre dann nicht nur der notwendige Schutz gewährleistet, sondern auch ein gewisses Vertrauen und eine Verlässlichkeit für den Verbraucher, die für den Einsatz von elektronischen Zahlungsmitteln unentbehrlich sind.

Denn wenn der Angriffsvektor weiter gefasst wird, bleibt das grundsätzliche Problem bestehen. Eine Erweiterung innerhalb einer Smartphone-App kann die implementierten Sicherheitsmechanismen unterlaufen. So wäre der weitgehende Einsatz von zusätzlichen Sicherungsmechanismen auf den Redirect-Bezahlseiten, wie beispielsweise CAPTCHAs, unerlässlich, um einem automatisierten und ungewünschten Zugriff aus einer App heraus vorzubeugen. Die Überprüfung der Bezahlseiten zeigte, dass im Juli 2017 die Variante, welche von der Telekom eingesetzt wird, im Vergleich zu denen der anderen Netzbetreiber technisch besser vor der untersuchten Missbrauchsoption schützt, da teilweise die genannten CAPTCHAS eingesetzt werden.

Darüber hinaus stehen in dem Geschäftsmodell Carrier Billing weitere Segmente zur Verfügung, in die kriminelle Aktivitäten verlagert werden können beziehungsweise die derzeit auch schon aktiv für kriminelle Aktivitäten genutzt werden. Vor allem Premium-SMS und Kurzwahlnummern sind zu nennen, die zu einem entsprechend missbräuchlichen Vertragsschluss führen können, wie es in den USA bereits zu beobachten war.[160] In Deutschland fallen außerdem häufiger kostenlose Smartphone-Apps auf, welche auf die Kontaktdaten der Nutzer zugreifen und hierüber teure SMS auf Kosten des Nutzers versenden.[161]

155 Siehe Bundesgesetzblatt (2017).
156 Gem. § 312d BGB in Verbindung mit Art. 246a EGBGB §3.
157 Siehe Kapitel 6.1.
158 Vgl. Deutscher Bundestag (2016).
159 Vgl. Stellungnahme der Clean Market Initiative, 25.11.2016.
160 Siehe Federal Communications Commission USA (2015) und Federal Trade Commission (o.J.).
161 Siehe https://www.teltarif.de/fake-apps-enlarven-geld-zurueck/news/67707.html

Netzbetreiber in der Pflicht?

In Bezug auf die „IT-Security“ der den Endkunden betreffenden Anwendungen ist generell auch ein proaktiveres Handeln von Seiten der Netzbetreiber im Sinne eines optimierten Verbraucherschutzes wünschenswert. Die als Angriffsvektor identifizierte Missbrauchstechnik ist im Webbereich eigentlich eine altbekannte Angriffsform, da sie bereits im Jahr 2008 eingängig besprochen wurde.[162] Wenn davon ausgegangen wird, dass technische Systeme nie zu 100 Prozent sicher sein können, so ist jedoch die Einhaltung eines Mindestschutzniveaus auf dem Stand der aktuellen Technik gegen standardisierte Angriffsvektoren durchaus möglich.[163] Wird der in der rechtlichen Analyse[164] diskutierte Punkt der Überwachungs- und Prüfpflichten auf den Vertragspartner in diesem Zusammenhang weiter gedacht, so ist dies insbesondere auch auf die technische Infrastruktur zu beziehen, über die Mobilfunkunternehmen in der Lage sind, Zugriff auf das Vermögen des Mobilfunkkunden zu nehmen. Die ermittelte Schadensumme deutet hingegen auf fehlende Anreize für eine funktionierende Selbstregulierung in dieser Branche hin. Vorteilhafter für den Verbraucher wäre demnach eine kontinuierliche Prüfung technischer Sicherungsmaßnahmen in Bezug auf die eingesetzten Verfahren durch eine anbieterunabhängige Instanz.

Opt-out als strukturelles Problem?

Unabhängig von den hier genannten Sicherungsoptionen bietet eine voraktivierte Drittanbietersperre für den Verbraucher in allen Segmenten des Carrier Billings erst einmal den einfachsten und umfassendsten Schutz. Inwiefern darüber informiert wird, wenn ein Mobilfunkvertrag abgeschlossen wird, ist unklar. In den stationären Shops der Mobilfunkanbieter geschieht dies häufig erst auf konkrete Nachfrage.[165] Dieser Aspekt ist in Bezug auf den Verbraucherschutz von äußerster Bedeutung. So muss der Verbraucher ausreichend über entsprechende Bezahlverfahren informiert sein, insbesondere dann, wenn darüber ohne weitere Authentifizierungsprozesse ein direkter Zugriff auf das eigene Portemonnaie möglich ist. Kritisch ist dies vor dem Hintergrund, dass der Verbraucher zur Nutzung eines Bezahlverfahrens dieses in der Regel beim Onlinekauf aktiv auswählen beziehungsweise durch einen vorherigen Registrierungsprozess überhaupt zur Nutzung aktiviert haben muss. Bei dem hier betrachteten Direct Billing-Verfahren geschieht dies allein durch den Abschluss eines Mobilfunkvertrages und den darin enthaltenen Inkassoklauseln. Der Verbraucher muss also, anders als gewohnt, das Bezahlverfahren aktiv abwählen, wenn er es nicht nutzen möchte, indem er eine Drittanbietersperre setzen lässt. Ist ihm die Bezahlmöglichkeit über die Mobilfunkanbieter nicht ausreichend bekannt, wird er dies ohne Hinweis oder qualifizierte Beratung, zum Beispiel in einem stationären Shop oder über die Internetpräsentation des Anbieters, nicht tun. Besteht nun die Möglichkeit eines einfachen systematischen technischen Missbrauchs, wird der Verbraucher gegebenenfalls geschädigt, ohne dass er dies im Vorwege überhaupt einschätzen und sich schützen kann.

Würde eine Drittanbietersperre, gegebenenfalls auch selektiv, standardmäßig voreingestellt, müssten die Anbieter, zum Beispiel im Rahmen des Vertragsschlusses, transparenter über dieses Bezahlverfahren informieren, um die Verbraucher von einer Aktivierung dieses Verfahrens zu überzeugen. Erst auf einer solchen Grundlage kann der Verbraucher dann, analog zu anderen Bezahlverfahren, eine fundierte und selbstbestimmte Entscheidung treffen.

162 Vgl. Hansen und Grossmann (2008).

163 Wenn auch für andere Bereiche, so finden sich vergleichbare Anforderungen zum Beispiel im Bundesdatenschutzgesetz (BDSG) oder in der Datenschutz-Grundverordnung (DSGVO).

164 Siehe 6.2.

165 Vgl. Stiftung Warentest (2016a), S. 55.

LITERATURVERZEICHNIS

Abraham, John/van der Lande, Justin (2013): Direct carrier billing: giving CSPs a share of the mobile payments market (Executive Summary). Präsentation. URL: http://www.analysysmason.com/Research/Content/Reports/direct-carrier-billing-Mar2013-RMA03/ [Stand: 14.07.2017].

Affil4you.com (2017a): URL-generator. URL: https://www.affil4you.com/index.php/de/kata-log-der-marketing-tools/url-generator [Stand: 14.07.2017].

Affil4you.com (2017b): iframe-Banner. URL: https://www.affil4you.com/index.php/de/kata-log-der-marketing-tools/iframe-banner [Stand: 14.07.2017].

Affil4you.com (2017c): BackBrowser. URL: https://www.affil4you.com/index.php/de/katalog-der-marketing-tools/backbrowser [Stand: 14.07.2017].

Apple (2016): Class UIWebView, Cupertino. URL: https://developer.apple.com/reference/uikit/uiwebview [Stand: 14.07.2017].

Arndt, Hans-Wolfgang/Fetzer, Thomas/Scherer, Joachim/Graulich, Kurt (2015): Telekommunikationsgesetz Kommentar, 2. Auflage, Berlin.

Bachfeld, Daniel (2010): Clickjacking für soziale Netze. In: Heise Online. URL: https://www.heise.de/security/meldung/Clickjacking-fuer-soziale-Netze-Likejacking-1014234.html [Stand: 14.07.2017].

BaRoss, John (2016): Direct carrier billing makes the transition from digital content to physical goods (Part 2). In: mobilepaymentstoday. URL: https://www.mobilepaymentstoday.com/articles/direct-carrier-billing-makes-the-transition-from-digital-content-to-physical-goods-part-2/ [Stand: 14.07.2017].

Bartsch, Steffen/Berger, Bernhard J./Bodden, Eric/Brucker, Achim D./Heider , Jens/Kus, Mehmet/Maseberg, Sönke/Sohr, Karsten/Volkamer, Melanie (2014): Zertifizierte Datensicherheit für Android-Anwendungen auf Basis statischer Programmanalysen. URL: https://www.secuso.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_SECUSO/Papers/Zertifizierte_Datensicherheit_fuer_Android-Anwendungen.pdf [Stand: 14.07.2017].

Beck'scher Online-Kommentar (2016): BGB, 41. Edition, München.

Beck'scher TKG-Kommentar (2013): Telekommunikationsgesetz, 4. Auflage, München.

Behrends, Sylvia/Joachimiak, Walter/Neuhäuser, Jenny (2016): Kapitel 6. Private Haushalte – Einkommen, Ausgaben, Ausstattung. In: Statistisches Bundesamt/Wissenschaftszentrum Berlin für Sozialforschung (Hrsg.): Datenreport 2016. Ein Sozialbericht für die Bundesrepublik Deutschland. URL: https://www.destatis.de/DE/Publikationen/Datenreport/Downloads/Datenreport2016.pdf?__blob=publicationFile [Stand: 14.07.2017].

Bitkom e.V. (2014): App-Markt wächst rasant. URL: https://www.bitkom.org/Presse/Presseinformation/App-Markt-waechst-rasant.html [Stand: 14.07.2017].

Bleich, Holger (2011): WAPzocke – Mit Smartphone-Abofallen wird weiter Kasse gemacht. In: Heise Online. URL: https://www.heise.de/ct/artikel/WAPzocke-1370330.html [Stand: 14.07.2017].

Böhle, Knut (2002): Internetzahlungssysteme in der Europäischen Union. In: Ketterer, Karl-Heinz/Stroborn, Karsten (Hrsg.): Handbuch ePayment: Zahlungsverkehr im Internet, Köln, S. 45-61.

Bootec Marketing Ltd (2017): Publishers. URL: https://www.brokerbabe.com/publishers [Stand: 14.07.2017].

Brisant (2016): In eine Abo-Falle getappt – und dann? URL: http://www.mdr.de/brisant/abo-falle-wap-billing-100.html [Stand: 14.07.2017].

Bundesamt für Sicherheit in der Informationstechnik (2013): Leitfaden zur Entwicklung sicherer Webanwendungen. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Web-anw_Auftragnehmer.pdf?__blob=publicationFile&v=1 [Stand: 14.07.2017].

Bundesamt für Sicherheit in der Informationstechnik (2015): Die Lage der IT-Sicherheit in Deutschland 2015, Bonn.

Bundesanstalt für Finanzdienstleistungsaufsicht (2009): Merkblatt Factoring. URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_090105_tatbestand_factoring.html [Stand: 14.07.2017].

Bundesgesetzblatt (2017): Drittes Gesetz zur Änderung des Telekommunikationsgesetzes, Bonn. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl117s1963.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1963.pdf%27%5D__1502711141614 [Stand: 14.07.2017].

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (2016): Meldepflicht - Informationen zur Anzeigepflicht der Anbieter von Telekommunikationsdiensten und Betreibern öffentlicher Telekommunikationsnetze. URL: http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/meldepflicht-node.html [Stand: 14.07.2017].

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (o. J.). URL: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/Deutschland/Mobilfunkteilnehmer/Mobilfunkteilnehmer_node.html [Stand: 14.07.2017 – derzeit nicht mehr aktiv].

Bundesverband E-Commerce und Versandhandel e. V. (2016): Interaktiver Handel in Deutschland, Ergebnisse 2015. URL: https://www.bevh.org/uploads/media/Auszug_u._besondere_Charts_der_bevh-Studie_Interaktiver_Handel_in_Deutschland_2015.pdf, abgerufen über URL: https://web.archive.org/web/20160409151301/https://www.bevh.org/uplo-ads/media/Auszug_u._besondere_Charts_der_bevh-Studie_Interaktiver_Han-del_in_Deutschland_2015.pdf [Stand: 14.07.2017].

Bundesverband Interaktive Unterhaltungssoftware e. V. (2016): Deutscher Markt für digitale Spiele im ersten Halbjahr 2016. URL: https://www.biu-online.de/marktdaten/deutscher-markt-fuer-digitale-spiele-im-ersten-halbjahr-2016/ [Stand: 14.07.2017].

Chaos Computer Club Hannover e. V. – CCC Hannover, Leitstelle 511 (2016): Was das neue Bahn-Wifi über seine Nutzer ausplaudert, Hannover. URL: https://hannover.ccc.de/~nexus/dbwifi/ [Stand: 14.07.2017].

Chaos Computer Club Hannover e. V. – CCC Hannover, Leitstelle 511 (2017): WLAN im ICE: Der Patch der Deutschen Bahn, der keiner war, Hannover. URL: https://www.ccc.de/de/updates/2017/bahn-wlan. [Stand: 14.07.2017].

Clean Market Initiative (2016a): Stellungnahme der Clean Market Initiative, 25.11.2016, St. Augustin.

Clean Market Initiative (2016b): Präsentation der Clean Market Initiative vom 30.08.2016, St. Augustin.

comScore (2016): Studie MobiLens.

Congstar (2016): Allgemeine Geschäftsbedingungen congstar Prepaid. URL: https://www.congstar.de/fileadmin/files_congstar/documents/2016/AGB/AGB_congstar_prepaid.pdf [Stand 01.08.2017].

Creswell, John W./Plano Clark, Vicki L. (2008): Chapter 3-4: Choosing a Mixed Methods Research Design. In: Creswell, John W./Plano Clark, Vicki L. (Hrsg.): Designing and Conducting Mixed Methods Research, London, S. 53-106.

Czumak, Mike (2013): Who do you trust? Cross-domain content extraction with Clickjacking. URL: http://www.securitysift.com/who-do-you-trust-cross-domain-content-extraction-with-clickjacking/ [Stand: 14.07.2017].

Dannenberg, Marius/Ulrich, Anja (2004): E-Payment und E-Billing: elektronische Bezahlsysteme für Mobilfunk und Internet, Wiesbaden.

Deutscher Bundestag (2011): Drucksache 17/5707. URL: http://dipbt.bundestag.de/dip21/btd/17/057/1705707.pdf [Stand: 14.07.2017].

Deutscher Bundestag (2015): Drucksache 18/6745. URL: https://dip21.bundestag.de/dip21/btd/18/067/1806745.pdf [Stand: 14.07.2017].

Deutscher Bundestag (2016): Drucksache 18/10480. URL: http://dip21.bundestag.de/dip21/btd/18/104/1810480.pdf [Stand 14.07.2017].

Deutscher Bundestag (2017): Drucksache 18/11811. URL: http://dip21.bundestag.de/dip21/btd/18/118/1811811.pdf [Stand 14.07.2017].

Deutscher Verband für Telekommunikation und Medien (2016): Click Fraud – Betrugsvorwürfe bedrohen die Branche. URL: http://web.archive.org/web/20160422081051/http://www.dvtm.net/ [Stand: 14.07.2017].

Empson, Rip (2013): Zuora Lands $50M From Next World, Paul Allen, Marc Benioff & More To Help Fuel The Rise Of The Subscription Economy. In: TechCrunch. URL: https://techcrunch.com/2013/09/05/zuora-lands-50m-from-next-world-paul-allen-marc-benioff-more-to-help-fuel-the-rise-of-the-subscription-economy/ [Stand: 14.07.2017].

Falk, Tomas (2012): Darstellung der weltweiten Mobile-Payment-Ansätze mit Smartphones und deren Adaptionspotenziale für Deutschland. Präsentation. URL: https://www.gs1-germany.de/fileadmin/gs1/basis_informationen/Forschungsergebnisse_Mobile_Payment_121221.pdf [Stand: 14.07.2017].

Federal Communications Commission USA (2015): Verizon & Sprint to pay $158 million to settle mobile cramming investigations, Washington. URL: https://apps.fcc.gov/edocs_public/attachmatch/DOC-333427A1.pdf [Stand: 14.07.2017].

Federal Trade Commission (o. J.): Mobile Cramming. URL: https://www.ftc.gov/news-events/media-resources/mobile-technology/mobile-cramming [Stand: 14.07.2017].

Felt, Adrienne Porter et al. (2012): Android Permissions: User Attention, Comprehension, and Behavior, Berkeley. URL: https://blues.cs.berkeley.edu/wp-content/uploads/2014/07/a3-felt.pdf [Stand: 14.07.2017].

Fenzl, Thomas/Mayring, Phillip (2014): Qualitative Inhaltsanalyse. In: Baur, Nina/Blasius, Jörg (Hrsg.): Handbuch Methoden der empirischen Sozialforschung, Wiesbaden, S. 543-558.

Garrett, Jesse James (2005): A New Approach to Web Applications. URL: https://web.archive.org/web/20080702075113/http://www.adaptivepath.com/ideas/essays/archives/000385.php [Stand: 14.07.2017].

Goldmedia GmbH Strategy Consulting (2016): Pay-VoD in Deutschland auf dem Weg zum Milliardenmarkt. URL: https://www.goldmedia.com/aktuelles/info/article/pay-vod-in-deutschland-auf-dem-weg-zum-milliardenmarkt/ [Stand: 14.07.2017].

Google (o. J.): WebView - public class WebView, Mountain View. URL: https://developer.android.com/reference/android/webkit/WebView.html [Stand: 14.07.2017].

Gutefrage.net (2016): Mobile666 Abo kündigen? Beitrag vom 19.09.2016. URL: http://www.gutefrage.net/frage/mobile666-abo-kuendigen [Stand: 14.07.2017].

Häder, Michael (2015): Empirische Sozialforschung - Eine Einführung, 3. Auflage, Wiesbaden.

Hansen, Robert/Grossmann, Jermiah (2008): Clickjacking. URL: http://www.sectheory.com/clickjacking.htm [Stand: 14.07.2017].

Heinze, Paulina (2017): So schützen Sie sich vor gefälschten Apps. URL: https://www.teltarif.de/fake-apps-enlarven-geld-zurueck/news/67707.html [Stand: 14.07.2017].

Hernandez, Will (2014): The overlooked mobile payment: direct carrier billing. In: mobilepaymentstoday. URL: https://www.mobilepaymentstoday.com/articles/the-overlooked-mobile-payment-direct-carrier-billing/ [Stand: 14.07.2017].

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (2016): Handbuch Multimedia-Recht, München.

Johnson, Omotunde E. G./Abrams, Richard K./Destresse, Jean-Marc/Lybek, Tonny/Roberts, Nicholas/Swinburne, Mark (1998): Payment Systems, Monetary Policy and the Role of the Central Bank, Washington DC.

Juniper Research/Dimoco (2013): Is mobile Operator Payment the Ideal Payment Method to Bill Digital Content? Whitepaper. URL: www.sfrpay.fr/content/download/1078/5586/version/1/file/DIMOCO_WP_FINAL 2013 (2).pdf [Stand: 14.07.2017].

Juniper Research/Dimoco (2016): The future of carrier billing in europe 3.0. URL: http://www.dimoco.eu/publications.html abgerufen über URL: https://web.ar-chive.org/web/20170219013522/http://www.dimoco.eu/publications.html [Stand: 14.07.2017].

Kantar TNS Infratest Dimap (2016): TNS Convergence Monitor. URL: https://www.tns-infratest.com/presse/pdf/Presse/2016-08-30_TNS_Infratest_ConvergenceMonitor_Smartphone_Charts.pdf [Stand: 14.07.2017].

Klees, Maria/Krüger, Malte/Eckstein, Aline (2013): Der Internetzahlungsverkehr aus Sicht der Verbraucher in D-A-CH - Ergebnisse der Umfrage IZV11, Köln.

Krüger, Malte (2016): Mobile Payments: The Second Wave. In: Górka, Jakub (Hrsg.): Transforming Payment Systems in Europe, Houndmills, Basingstoke, Hampshire.

Looper, Jen (2015): What is a WebView? URL: http://developer.telerik.com/featured/what-is-a-webview/ [Stand: 14.07.2017].

Mayring, Philipp (2014): Qualitative content analysis: theoretical foundation, basic procedures and software solution, Klagenfurt. URL: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-395173 [Stand: 14.07.2017].

mdk GmbH (2016a), mdk Gesellschaft für Entwicklung und Betrieb technischer Mehrwert-diensteplattformen mbH: Kompetenzzentrum Mehrwertdienste: Einheitliche Bezahlmaske. URL: http://mehrwertdienstekompetenz.de/?page_id=61, abgerufen über URL: https://web.archive.org/web/20161026112714/http://mehrwertdienstekompe-tenz.de/?page_id=61 [Stand 14.07.2017].

mdk GmbH (2016b), mdk Gesellschaft für Entwicklung und Betrieb technischer Mehrwert-diensteplattformen mbH: Kompetenzzentrum Mehrwertdienste: Einheitliche Bezahlmaske. URL: http://mehrwertdienstekompetenz.de/?page_id=12#1.4, abgerufen über URL: https://web.archive.org/web/20161026120401/http://mehrwertdienstekompe-tenz.de/?page_id=12 [Stand 14.07.2017].

mdr (2016): In eine Abo-Falle getappt – und dann? URL: http://www.mdr.de/brisant/abo-falle-wap-billing-100.html [Stand: 14.07.2017].

Moneyhouse AG (2017). URL: https://www.moneyhouse.ch/de/company/clickattack-ag-5756627881# [Stand: 14.07.2017].

Net mobile AG (2016). URL: https://www.net-mobile.com/de/unternehmen/investoren/ ab-gerufen über URL: https://web.archive.org/web/20160729194906/https://www.net-mo-bile.com/de/unternehmen/investoren/ [Stand: 14.07.2017].

NTH Group (2015): Business goes mobile. URL: http://topchoiceclub.com/app/uploads/2015/01/NTH_Group.pdf [Stand: 14.07.2017].

O2 Online (2017): Beispielrechnung. URL: https://static2.09.de/blob/11396118/v=9/Binary/02-more-direct2bill-beispielrechnung.pdf [Stand: 14.07.2017].

OWASP (2016): Clickjacking. URL: https://www.owasp.org/index.php/Testing_for_Click-jacking_(OTG-CLIENT-009) [Stand: 14.07.2017].

OWASP (2017): Clickjacking. URL: https://www.owasp.org/index.php/Clickjacking [Stand: 14.07.2017].

Rosenthal, Mark (2017): Wie Kunden reingelegt werden. In: ZDFzoom: Die Handy-Abo-Falle. URL: http://www.heute.de/zdfzoom-die-handy-abo-falle-wie-kunden-reingelegt-werden-47268382.html [Stand 14.07.2017].

Sauter, Martin (2011): Grundkurs Mobile Kommunikationssysteme, 4. Auflage, Wiesbaden.

Schalling, Daniel/Richter, Hannes/Fries, Johannes/von der Burg, Katja/Fischer, Luisa/Kärner, Stefan (2015): Affiliate Marketing – Ein Leitfaden für Affiliates und Merchants, Version 2.0, Leipzig.

Schmidt, Jürgen (2009): Twitter-Wurm „Don‘t Click“ verbreitet sich im Twitter-Space [Update]. In: Heise-Online. URL: https://www.heise.de/security/meldung/Twitter-Wurm-Don-t-Click-verbreitet-sich-im-Twitter-Space-Update-195344.html [Stand: 14.07.2017].

Schneider, Wolfgang (2008): Ergonomische Gestaltung von Benutzungsschnittstellen – Kommentar zur Grundsatznorm DIN EN ISO 9241-110, 2. Auflage, Berlin.

Scholz, Heike (2016): NFC City Berlin: Bilanz nach einem Jahr, in mobile zeitgeist. URL: https://www.mobile-zeitgeist.com/nfc-city-berlin-bilanz-nach-einem-jahr/ [Stand: 14.07.2017].

Spindler, Gerald/Schuster, Fabian (2015): Recht der elektronischen Medien: Kommentar, 3. Auflage, München.

Stefanko, Lukas (2015): Android trojan drops in, despite Google's Bouncer. URL: http://www.welivesecurity.com/2015/09/22/android-trojan-drops-in-despite-googles-bouncer/ [Stand: 14.07.2017].

Stiftung Warentest (2016a): Beratung in Mobilfunkshops, Test 5/2016, S. 54-57.

Stiftung Warentest (2016b): Handy-Abofallen: Wie Sie sich schützen und gegen Abbuchungen wehren. URL: https://www.test.de/Handy-Abofallen-Wie-Sie-sich-schuetzen-und-gegen-Abbuchungen-wehren-5069366-0/ [Stand 14.07.2017].

Telefónica Germany GmbH & Co. OHG (2015): Allgemeine Geschäftsbedingungen der Telefónica Germany GmbH & Co. OHG für „blauworld classic" und „blauworld plus". URL: http://www.blauworld.de/cms/blauworldRelaunch/documents/blauworld_agb.pdf [Stand: 14.07.2017].

Verbraucherzentrale Bundesverband (2003): Kinder und Jugendliche durch Werbekompetenz schützen – Hintergrundpapier zur Kinderkampagne, Berlin. URL: http://www.vzbv.de/sites/default/files/mediapics/kinderkampagne_hintergrundpapier_10_2003.pdf [Stand: 14.07.2017].

Verbraucherzentrale Bundesverband (2011): Kostenfallen endlich in der Falle. URL: http://www.vzbv.de/pressemitteilung/kostenfallen-endlich-der-falle [Stand 14.07.2017].

Verbraucherzentrale Bundesverband (2016a): Abzocke per Smartphone: Hilfe bei ungewollten Abos. URL: https://www.verbraucherzentrale.de/smartphoneabzocke [Stand: 14.07.2017].

Verbraucherzentrale Bundesverband (2016b): Selbstverständnis zu Untersuchungen im Marktwächter Digitale Welt: Angewandte Forschung aus Verbrauchersicht.

Vierthaler, Johann (2016): Technisches Kurzgutachten: Missbrauchsmöglichkeiten in Bezug auf Redirect-basierte Schutzmaßnahmen für Mehrwert-Dienste-Bezahlverfahren, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC, München.

Vierthaler, Johann (2017): Delta-Evaluation von Missbrauchsmöglichkeiten in Bezug auf Redirect-basierte Schutzmaßnahmen für Mehrwert-Dienste-Bezahlverfahren, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC, München.

Vodafone GmbH (2016): Allgemeine Geschäftsbedingungen für Vodafone-Dienstleistungen (AGB). URL: https://www.vodafone.de/infofaxe/203.pdf [Stand: 01.08.2017].

W2M GmbH (2016): FAQ. URL: http://affiliate.w2mobile.com/de/ [Stand: 14.07.2017].

Weidner, Markus (2016): WhatsApp Gold Edition: Malware statt Premium-Features. URL: https://www.teltarif.de/warnung-whatsapp-gold-edition/news/64068.html [Stand: 14.07.2017].

Whitwam, Ryan (2012): Circumventing Google's Bouncer, Android's anti-malware system. URL: http://www.extremetech.com/computing/130424-circumventing-googles-bouncer-androids-anti-malware-system [Stand: 14.07.2017].

Wijesekera, Primal et al. (2015): Android Permissions Remystified: A Field Study on Contextual Integrity, Washington. URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-wijesekera.pdf [Stand: 14.07.2017].

Zeit Online (2015): Verbraucherschützer warnen vor WhatsApp-Fallen. URL: http://www.zeit.de/digital/mobil/2015-06/whatsapp-verbraucherschutz-warnung-betrug-wap-billing [Stand: 14.07.2017].

Zuora Inc. (2017): The world is shifting to a new kind of business model. URL: https://www.zuora.com/vision/subscription-economy/ [Stand: 14.07.2017].

ABKÜRZUNGSVERZEICHNIS

A

AG – Arbeitsgericht

AGB – Allgemeine Geschäftsbedingungen

App – Anwendungssoftware für Smartphone oder Tablet

B

BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht

BGB – Bürgerliches Gesetzbuch

BGH – Bundesgerichtshof

C

CATI – Computer Assisted Telephone Interview

CAPTCHAS – Completely Automated Public Turing test to tell Computers and Humans Apart

CSRF – Cross-Site-Request-Forgery

D

D-A-CH-Region – Region deutschsprachiger Länder, D für Deutschland, A für Österreich und CH für die Schweiz

DIN EN ISO – DIN steht für Deutsches Institut für Normung, EN für Europäische Norm und ISO für International Organization for Standardization

DVTM – Deutscher Verband für Telekommunikation und Medien e. V.

F

forsa – forsa main Marktinformationssysteme GmbH

FWN – Frühwarnnetzwerk

H

HGB – Handelsgesetzbuch

HTTP – Hypertext Transfer Protocol

HTML – Hypertext Markup Language

I

ISP – Internet Service Provider

IPv4, IPv6 – Internet Protocol Version 4, Internet Protocol Version 6

K

KWG – Gesetz über das Kreditwesen

KWN – Kurzwahlnummer

L

LG – Landgericht

M

MSISDN – Mobile Subscriber Integrated Services Digital Network Number

N

NFC – Near Field Communication

O

OLG – Oberlandesgericht

OWASP – Open Web Application Security Project

P

POS – Point of Sale – Stationärer Handel/Ladengeschäft

S

SIM – Subscriber Identity Module (Teilnehmer-Identitätsmodul)

SMS – Short Message Service (Kurznachrichtendienst)

StGB – Strafgesetzbuch

T

TAN – Transaktionsnummer

TK – Telekommunikation

TKG – Telekommunikationsgesetz

TMG – Telemediengesetz

U

UKlaG – Unterlassungsklagengesetz

URL – Uniform Resource Locator

UWG – Gesetz gegen den unlauteren Wettbewerb

V

vzbv – Verbraucherzentrale Bundesverband

W

WAP – Wireless Application Protocol

WLAN – Wireless Local Area Network

Z

ZAG – Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz)

GLOSSAR

A

Affiliates – Ein Affiliate wird im Onlinemarketing als der Vertriebspartner eines Verkäufers/Händlers (engl. merchant) bezeichnet. Dazu bindet der Affiliate auf der eigenen Webseite beispielsweise einen Werbebanner oder einen Link ein, die auf die Seite des Verkäufers verweisen. Im Gegenzug erhält der Affiliate eine Provision, die sich an unterschiedlichen, im Vorwege definierten Kriterien orientiert (Anzahl der Werbeeinblendungen, Zeitraum der geschalteten Werbung, Klick, Bestellung oder hinzu gewonnener Kontakt).[166]

Aggregator – Der Aggregator, auch Enabler oder Billing-Carrier genannt, ist das Bindeglied zwischen Drittanbieter und Mobilfunkunternehmen. Für die Mobilfunkunternehmen organisiert er die Drittanbieter, meldet diese und deren Angebote über ein dafür vorgesehenes System bei den Mobilfunkunternehmen an, damit sie über deren Rechnung ihre Leistungen abbuchen können. Den Drittanbietern gegenüber nimmt der Aggregator die Funktion eines Payment-Service-Providers, also eines Bezahldienstleisters, ein. Im Zusammenhang mit dieser Funktion wickeln diese Unternehmen u.a. den eigentlichen Buchungsprozess der Drittanbieterleistung technisch über eine eigene Infrastruktur ab.

ARPU – Average Revenue per User – durchschnittlicher monatlicher Umsatz pro Kunde

B

Browser-Addon – Ein Browser-Addon ist eine optionale Browsererweiterung, die Nutzer in der Regel manuell installieren können. Diese Addons setzen auf der Browsersoftware auf und erweitern dessen Funktionsumfang. Das können Designs sein, die Einfluss auf die Optik des Browsers haben, es können aber auch Programme sein, die Werbung blockieren oder bestimmte Skriptsprachen unterdrücken.

Billing-Carrier – siehe Aggregator

Butt/pocket calls – Hosentaschenanruf. Unbewusster Anruf bei einer Kurzwahlnummer, die kostenpflichtig ist und durch die Berührung mit der Hose, dem Gesäß hervorgerufen worden ist.

C

CAPTCHAS – Technik, um automatisierte Aufrufe bzw. Eingaben bei Formularen und anderen Aktionsflächen auf Webanwendungen zu unterbinden.

Carrier Billing – Geschäftsmodell, über das bestimmte Transaktionen, in der Regel der Kauf digitaler Güter mit dem Mobiltelefon, über die Rechnung des Mobilfunkanbieters abgebucht werden.

Check-Out-Prozess – Der Check-Out-Prozess beschreibt den Weg, den ein Nutzer gehen muss, wenn er in einem Online-Shop seine Bestellung abschließt. In der Regel startet dieser Prozess mit dem Button unter der Übersicht des Warenkorbs und beinhaltet in der Regel die Schritte Versandinformationen eingeben, Versandmethode auswählen, Bezahlverfahren auswählen, Bestellübersicht und Bestellung durchführen.

Clean Market Initiative – Gemeinsamen Qualitätsoffensive deutscher Mobilfunknetzbetreiber, deren Ziel es ist, einheitliche, kundenfreundliche Regelungen und Standards für das Bezahlen über die Mobilfunkrechnung im Markt zu etablieren.

Clickjacking – auch bekannt unter dem Begriff „UI redress attack“, beschreibt einen Angriff im Webbrowser. Der Angreifer setzt auf einer Webseite mehrere transparente oder undurchsichtige Schichten ein, um den Benutzer zu einem Klick auf einen Button oder einen Link zu veranlassen, deren Aktion dann auf einer anderen Seite ausgeführt wird.

CSRF – Cross-Site-Request-Forgery – Angriffsart, die gültige Sitzungsdaten zwischen einem anzugreifenden Server und dem Browser eines Opfers ausnutzt, um schädliche Anfragen zu versenden.

CSRF-Token – Eine Zeichenkette, die bei jedem Webseitenaufruf neu und zufällig generiert wird. Diese Tokens

166 Vgl. http://www.onlinemarketing-praxis.de/glossar/affiliate-publisher-partner, abgerufen am 10.01.2017

werden auf dem Server abgelegt und derart in die Webseiten eingebettet, dass sie bei jeder Anfrage mitgeschickt werden. Bei einer späteren Bearbeitung durch den Server kann dieser dann an Hand verschiedener Kriterien überprüfen, ob der gelieferte Token gültig ist und die gewünschte Aktion ausführen. CSRF-Token stellen einen Schutz gegen CSRF-Angriffe dar.

D

Direct Billing – In dieser Studie wird von Direct Billing gesprochen, wenn es um die konkrete technische Ausgestaltung des Bezahlverfahrens über das mobile Internet geht, unabhängig davon, ob dies über eine Webseite oder eine App auf dem Smartphone implementiert ist. Um zu bezahlen, muss der Nutzer auf einen beziehungsweise mehrere Button im Rahmen der entsprechenden Anwendung klicken, zum Beispiel dem Browser.

Direct Operator Billing – siehe Carrier Billing

Dual-Frame-Ansatz – Stichprobenerhebung aus zwei Auswahlrahmen – einer Festnetzstichprobe sowie einer Mobilfunkstichprobe. Der Hauptvorteil liegt in der Berücksichtigung der sogenannten „Mobile-Onlys", also Personen, die ausschließlich über ihr Mobiltelefon erreichbar sind und über keinen Festnetzanschluss verfügen.

Dynamic Class Loading – Dynamic class loading ermöglicht einer Anwendung ihr Verhalten während des Betriebes zu ändern. Diese Technik wird häufig in Android Apps verwendet, insbesondere auch von Entwicklern, die Malware programmieren.[167]

E

Enabler – siehe Aggregator

F

Factoring – Factoring ist der laufende Ankauf von Forderungen aus Lieferungen oder Leistungen des Factoringkunden (= „Anschlusskunden" oder „Verkäufers") durch den Factor („Käufer") nach Maßgabe eines Rahmenvertrags. Je nach vertraglicher Ausgestaltung kann der Anschlusskunde dabei dem Factor die gesamte Debitorenbuchhaltung, einschließlich des Inkasso- und Mahnwesens und des gerichtlichen Forderungseinzugs, übertragen.[168]

Framebusting – Techniken, die verhindern, dass Webseiten via frame/iframe in andere Webseiten geladen werden können.

Frühwarnnetzwerk – Beim FWN des Marktwächters handelt es sich um ein Erfassungs- und Analysesystem für auffällige Sachverhalte aus der Verbraucherberatung. Grundlage stellt eine ausführliche Sachverhaltsschilderung durch Beratungskräfte dar, die eine Kategorisierung sowie eine anschließende qualitative Analyse ermöglicht. Eine Quantifizierung der Daten aus dem FWN heraus bzw. ein Rückschluss auf die Häufigkeit des Vorkommens in der Verbraucherberatung insgesamt ist jedoch nicht möglich.

H

Header (HTTP) – Der Header, der während einer Internetsitzung übertragen wird, kann sinnbildlich als Kopf eines Datenblocks angesehen werden, der Zusatzinformationen mitliefert, zum Beispiel die IP-Adresse der Station, die das Datenpaket abgeschickt hat und die IP-Adresse der Station, für die das Paket bestimmt ist.

Header Enrichment – Header Enrichment beziehungsweise HTTP Header Enrichment bezeichnet das Hinzufügen von Informationen, zum Beispiel die MSISDN, zum HTTP Header, so dass die Inanspruchnahme eines Web Services einem Mobilfunknutzer zugeordnet werden kann.

HTTP-Response-Header – Der HTTP-Response-Header ist Bestandteil des Hypertext Transfer Protocol (HTTP)-Protokollheaders. Über die Felder des Response-Headers kann der Server weitere Informationen übertragen, wie zum Beispiel Informationen zum Sicherheitskonzept oder eine andere URL, zu der Nutzer weitergeleitet werden sollen.

I

iframe – Ein iframe ist ein HTML-Element, das zur Strukturierung von Webseiten genutzt wird. Über einen iframe

167 Siehe Ahmad et al. (2016), S. 119.

168 Siehe Bafin (2009).

ist es möglich, Inhalte anderer Webseiten einzubinden, zum Beispiel um einen Bezahlvorgang auf der technischen Infrastruktur eines Payment-Service-Providers durchzuführen.

L

Last-Birthday-Methode – Die Interviewer ermitteln die zu befragende Person in Mehrpersonenhaushalten mit Hilfe der sogenannten Geburtstagsmethode, um eine Zufallsstichprobe zu gewährleisten. Dazu fragt der Interviewer diejenige Person, die nach der Haushaltsanwahl als erstes ans Telefon geht, wer im Haushalt als letzter Geburtstag (Last-Birthday) hatte und mindestens 14 Jahre alt ist.

Library – In der Programmierung wird unter einer Library beziehungsweise einer Programmbibliothek eine Sammlung von Unterprogrammen verstanden, auf die andere Programmkomponenten zugreifen. Diese können zum Beispiel auch in einem Verzeichnis gesammelt sein.

M

Malvertising – Dieser Begriff setzt sich aus „Malware“ für schädliche Software und „Advertising“ für Werbung zusammen. Diese „schädliche Online-Werbung“ wird in der Regel dazu benutzt, Schadprogramme zu verbreiten.

Man-in-the-Middle-Angriff – Bei Man-in-the-Middle-Angriffen wird die Kommunikation zwischen zwei Parteien abgehört. Am praktischen Beispiel ist das Ziel während einer http-Transaktion die TCP-Verbindung, also das Übertragungssteuerungsprotokoll, zwischen Klienten und Server. Mittels verschiedener Techniken trennt der Angreifer die ursprüngliche TCP-Verbindung und übersetzt diese in zwei neue Verbindungen – die Erste liegt dabei zwischen dem Klienten und den Angreifer, die zweite Leitung verbindet den Angreifer wiederum mit dem Server. Ist die ursprüngliche Verbindung einmal getrennt, fungiert der Angreifer als ein in der Mitte der Kommunikation stehender und bevollmächtigter Akteur, der die übermittelten Daten lesen und modifizieren sowie neue Daten einfügen kann.

Micropayment-Bereich – Kleinbetragzahlung, Mikrozahlung: Bezahlverfahren geringer Summen.

MNO – Mobile Network Operator – Mobilfunknetzbetreiber, d.h. ein Unternehmen, das öffentliche Mobilfunkdienste anbietet und im deutschen Hoheitsgebiet dazu bei der Bundesnetzagentur lizensiert ist. Z. T. wird der Begriff „Carrier“ auch synonym zu MNO verwendet. In Deutschland gibt es derzeit drei MNOs: Telefónica (O2 und E-Plus), Telekom und vodafone.

MNO-Redirect – siehe Redirect

Mpass – Mobiles Internet-Bezahlsystem. Wurde im September 2016 eingestellt.

MVNO – Mobile Virtual Network Operator – virtuelle Netzbetreiber. In Abgrenzung zu den MNO handelt es sich bei den virtuellen Netzbetreibern um reine Wiederverkäufer der MNO-Leistungen, d.h. die MVNO betreiben keine eigenen Mobilfunknetze. In Deutschland zählen dazu zum Beispiel mobilcom-debitel, congstar, ALDITalk etc.

MSISDN – Die eigentliche Telefonnummer eines Teilnehmers, die auch Mobile Subscriber ISDN Number (MSISDN) genannt wird[169].

N

Near Field Communication (NFC) – Funkstandard zur drahtlosen Datenübertragung, wobei sich beide Geräte in unmittelbarere Nähe zueinander befinden müssen.

O

One-Click Payment – Unter One-Click-Payment wird in diesem Zusammenhang ein Bezahlvorgang im Internet verstanden, der ausschließlich auf einem einzigen Klick basiert, ohne dass sich der Nutzer weiter authentifizieren muss, zum Beispiel durch einen Login.

Opt-in – Das Opt-in-Verfahren besagt, dass eine ausdrückliche Erklärung des Verbrauchers, zum Beispiel in Form einer Unterschrift oder durch Ausfüllen eines Formulars im Internet, für die Benutzung eines Verfahrens vorliegen muss. Liegt keine Einwilligung des Verbrauchers vor, so kann er nicht an dem Verfahren teilnehmen.

169 Siehe Sauter (2011), S. 24.

OTT-Dienste – Over-the-Top Dienste – OTT-Dienste werden über das Internet ausgeliefert und stehen teilweise in Konkurrenz zu klassischen Telekommunikationsdiensten. Sie werden unterschieden in OTT-Kommunikations- und OTT-Inhaltsdienste. OTT-Kommunikationsdienste, wie zum Beispiel Messagingdienste oder Internettelefonie, stehen in einer direkten Konkurrenzbeziehung zur klassischen SMS oder Sprachtelefonie. Demgegenüber sind OTT-Kommunikationsdienste, beispielsweise Suchmaschinen oder Angebote aus dem Social-Web, eher in einem komplementären Verhältnis zu klassischen Telekommunikationsdiensten zu sehen.

OWASP – Open Web Application Security Project – Hierbei handelt es sich um eine weltweite Non-Profit-Organisation, welche sich mit der Verbesserung von Softwaresicherheit beschäftigt. Die Organisation schreibt: "Es ist unsere Aufgabe, das Thema Softwaresicherheit sichtbar zu machen, damit Individuen und Organisationen die Möglichkeit haben, fundierte Entscheidungen zu treffen. OWASP ist dabei in der besonderen Lage, Einzelpersonen, Unternehmen, Universitäten, Behörden und anderen Organisationen weltweit unparteiische und praxisnahe Informationen über AppSec zur Verfügung zu stellen. Als Gemeinschaft von gleichgesinnten Experten erstellt OWASP sowohl Softwarewerkzeuge als auch wissensbasierte Unterlagen über Anwendungssicherheit."

P

Payment-Service-Provider – Zu Deutsch: Zahlungsdienstleister. „Payment-Service-Provider (PSP) sind Unternehmen, die sich im E- Commerce Bereich auf die technische Anbindung und die Transaktionsabwicklung von Bezahllösungen spezialisiert haben. PSP bieten damit sozusagen die „virtuelle Kasse" für das Internet an und integrieren die gewünschten Bezahlsysteme in Online-Shops. Damit ersparen sich Online-Händler die direkte Anbindung an alle einzelnen Zahlungsverkehrssysteme, sämtliche Zahlungsvorgänge laufen über eine Schnittstelle. Payment-Service-Provider bieten zumeist eine Vielzahl von unterschiedlichen Zahlungsmethoden, ob Kreditkarten, eps Online-Überweisung, Wallet-Lösungen wie PayPal, ELV, mobiles Bezahlen über paybox, paysafecard oder Qick und unterstützen Webshopbetreiber bei der Auswahl der auf ihren Bedarf individuell zugeschnittenen Bezahlsysteme."[170]

Prepaidvertrag – Vertragsart basierend auf dem Gebrauch von sogenannten Prepaidkarten. „Für die Verwendung von Prepaidkarten erwirbt der Kunde im Voraus ein Guthaben, das für die Abrechnung von Gesprächen, SMS und MMS sowie mobilem Internet genutzt werden kann."[171]

Point of Sale (POS) – Verkaufs- oder Einkaufsstelle.

Postpaid-Vertrag – Vertragsart mit nachträglicher Rechnungslegung.

R

Redirect – Im Internet bezeichnet ein Redirect eine Um- oder Weiterleitung auf eine andere Internetadresse, auf deren Ziel der Nutzer je nach Art der technischen Umsetzung zumeist keinen Einfluss hat. Im Zusammenhang mit dieser Untersuchung ist unter Redirect die Weiterleitung von der Webseite des Drittanbieters auf eine Bezahlseite des Netzbetreibers beziehungsweise des MVNO gemeint.

Redressment – Redressement bezeichnet ein Verfahren in der Marktforschung, nach dem die durchgeführten Interviews per Gewichtung an die normale Bevölkerungsstruktur, basierend auf der amtlichen Statistik, angepasst werden.

Remote payment – Zu Deutsch: Fernzahlung. Eine Zahlungsart, welche durch das Senden eines Zahlungsauftrages oder über ein Zahlungsinstrument (z. B. via E-Mail) ausgeführt wird.[172]

Response-Header – siehe HTTP-Response-Header

S

Same-Origin-Policy – Die Same-Origin-Policy regelt den skriptseitigen Zugriff (zum Beispiel mittels Javascript, HTML und Actionscript) von einer im Browser geladenen Webseite auf Inhalte einer anderen Webseite.

SMS – Short Message Service, Kurznachrichtendienst

SMS-TAN-Verfahren – siehe Web-Billing

170 https://www.wko.at/Content.Node/branchen/oe/zahlungsverkehr-e-m-commerce/payment_service_provider.html; 17.02.2017

171 https://www.teltarif.de/mobilfunk/prepaid/

172 Siehe Johnson et al. (1998), S. 244.

Spam – Unerwünschte Mitteilung zu Werbezwecken

Social Engineering – Angreifer versuchen das persönliche Umfeld des Opfers auszukundschaften und diese anschließend über gezielte Aktionen dazu zu verleiten, bestehende Schutzmechanismen außer Acht zu lassen oder unbewusst Schadprogramme, beispielsweise auf ihrem Smartphone, zu installieren. Dabei werden durch die Angreifer menschliche Schwächen wie zum Beispiel Vertrauen, Neugier oder Respekt angesprochen.[173]

Styleguide – In dem genannten Zusammenhang: Vorgaben zur strukturellen und optischen Umsetzung von Webanwendungen

T

Template – Technische Formatvorlage, über das Inhalte auf einer Webseite im Internet standardisiert dargestellt werden.

TNB – Teilnehmernetzbetreiber – „Der Begriff des Teilnehmernetzbetreibers ist zwar weder im TKG 2004 noch im TKG 2012 definiert. Da aber „Teilnehmernetz“ als Definition in § 3 Nr. 27 TKGverankert ist, kann davon ausgegangen werden, dass hierunter Teilnehmer zu verstehen sind, die ein diesbezügliches Telekommunikationsnetz betreiben.“[174]

U

URL – Uniform Resource Locator – eine „eindeutige Identifikation bzw. Adresse eines HTML-Dokuments im Internet. Die URL setzt sich aus der Domäne und der Angabe des Ortes des Dokuments auf dem Server zusammen.“[175]

Usability – Zu Deutsch: Benutzerfreundlichkeit. Diese ist „Merkmal der Softwarequalität. Die Eigenschaft eines Softwareprodukts, bes. eines Dialogsystems, auf die Anforderung des Endbenutzers zugeschnitten zu sein. Das Softwareprodukt soll sich den Bedürfnissen der jeweiligen Benutzerkategorie entsprechend verhalten, der Vorbildung und Intention der Benutzer angemessene Ausdrucks- und Interaktionsformen vorsehen und leicht handhabbar sein. Die Benutzerfreundlichkeit wird intensiv innerhalb der Software-Ergonomie untersucht.“[176]

V

VNB – Verbindungsnetzbetreiber – „Der Gesetzgeber hat im Rahmen des TKG 2004 auf den Begriff des Verbindungsnetzbetreibers verzichtet. § 45h Abs. 4 TKG alte Fassung nahm diesen Begriff wieder auf. In der aktuellen Fassung 2012 hat der Gesetzgeber den Begriff wieder durch „andere beteiligte Anbieter“ ersetzt. Hierbei handelt es sich aber lediglich um eine redaktionelle Anpassung.158 § 45 h Abs. 4 TKG trägt dem Umstand Rechnung, dass bestimmte Leistungen (z. B. Call-by-Call und Mehrwertdienste die im Offline-Billing-Verfahren abgerechnet werden) regelmäßig bei einem Verbindungsnetzbetreiber realisiert werden, der über die erforderlichen Infrastrukturen verfügt. Dies schließt nicht aus, dass Anbieter die Funktionen eines Teilnehmernetzbetreibers oder Verbindungsnetzbetreibers in sich vereinen. Zur Begriffsbestimmung ist aufgrund der fehlenden Definition in § 3 auf das TKG 1996 zurückzugreifen. Danach ist ein Verbindungsnetz ein Telekommunikationsnetz, das keine Teilnehmeranschlüsse aufweist und Teilnehmernetze miteinander verbindet (§ 3 Nr. 23 TKG 1996); ferner auch dann, wenn das Telekommunikationsnetz lediglich der Terminierung von Zielen auf technischen Plattformen dient.“[177]

W

WAP-Billing – WAP-Billing bezeichnet die Rechnungstellung von digitalen Gütern, die über das mobile Endgerät von dafür vorgesehenen Internetseiten heruntergeladen oder dort angesehen werden. Die Verbindung zum Aufruf dieser Internetseiten wird über das WAP-Protokoll realisiert und auch die Seiten selbst sind in der Regel für dieses Protokoll ausgelegt.

Webview – Eine Webview ist eine Komponente innerhalb des jeweiligen „Programmiergerüstes“, auf denen Apps aufbauen, das die Darstellung und Interaktion mit Webseiten innerhalb der installierten Applikation ermöglicht.

Web-Billing – In Abgrenzung vom hier verwendeten Begriff des Direct Billings muss beim Web-Billing die

173 Siehe BSI 2015, S. 24.
174 Geppert (2013), TKG § 45 h Rn. 61
175 http://wirtschaftslexikon.gabler.de/Definition/url.html
176 http://wirtschaftslexikon.gabler.de/Definition/benutzerfreundlichkeit.html
177 Siehe Geppert (2013), TKG § 45 h Rn. 62.

MSISDN manuell in ein Formular eingegeben werden. Anschließend erhält der Nutzer eine TAN via SMS, die er wiederum in ein Formular eingeben muss, um seine Leistung freizuschalten, die dann über die Mobilfunkrechnung abgebucht wird.

Web/TAN Flow – siehe Web-Billing

XmlHttpRequest (asynchrone) – Asynchrone XmlHttp Requests ermöglichen die Kommunikation zwischen dem Webbrowser des Benutzers und einem Server über zwischengeschaltete Techniken, ohne dass der Benutzer seine Interaktion mit der Webanwendung unterbrechen muss, zum Beispiel weil eine neue Seite geladen werden muss oder eine Sanduhr angezeigt wird.

IMPRESSUM

Herausgeber
Verbraucherzentrale Schleswig-Holstein e. V.
Geschäftsführer Stefan Bock
Hopfenstraße 29
24103 Kiel
Tel. (0431) 590 99-0
Fax (0431) 590 99-77
E-Mail: marktwaechter@vzsh.de

Autoren: Tom Janneck, Alexander Grams, Kerstin Heidt, Samanta Hoffmann, Per Prins

Titelillustration: shutterstock/LuckyVector, Noun Project (Icons)
Gestaltung: Birgit Hirschmann
Druck: Königsdruck – Printmedien und digitale Dienste GmbH

Stand: September 2017
Gedruckt auf 100 Prozent Recyclingpapier

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

verbraucherzentrale