Bernd Otter

»Räuber und Gendarm

Überall dort, wo wir andere für eine Leistung bezahlen, besteht auch immer potentiell die Gefahr, ausgetrickst zu werden. Bernd Otter, Experte für Betrugserkennung, zeigt alles über eine der hinterhältigsten Betrugstechniken im Affiliate-Marketing und erklärt, warum vermutlich jeder zweite Shop in Deutschland davon betroffen ist - und wie viel Geld dabei auf dem Spiel steht!

Um das Thema gleich zu Beginn greifbarer werden zu lassen, stelle man sich bitte das folgende Szenario aus dem Stationärhandel vor:

Einführung

Sie sind Besitzer eines Ladens in einem großen Einkaufszentrum und verkaufen dort Ihre Waren. Ihr Geschäft läuft sehr gut: Sie bieten hochwertige Produkte zu konkurrenzfähigen Preisen an und haben sich mittlerweile ein angesehenes Markenimage in Ihrer Umgebung aufgebaut. Ein neuer Geschäftspartner, nennen wir ihn Herr Müller, kommt auf Sie zu und bietet Ihnen Folgendes an: Er verteilt Flyer von Ihnen an einem entfernten Ende des Gebäudes, um die Passanten dort auf Sie aufmerksam zu machen und zu einem Besuch Ihres Geschäftes zu bewegen. Im Gegenzug erhält Herr Müller eine kleine Provision für jeden Kunden, der mit genanntem Flyer Ihr Geschäft betritt und etwas bei Ihnen einkauft. Klingt nach einem vernünftigen Geschäftsmodell? Einverstanden.

Sie gehen diese Kooperation ein und nach einer kurzen Anlaufphase läuft alles wie geschmiert: Immer wieder kommen durch Herrn Müller „geworbene" Kunden in den Laden und kaufen etwas bei Ihnen. Von Monat zu Monat werden es immer mehr „Flyerkunden" und Sie sind von der Sache begeistert. Sie fragen sich, warum Sie nicht schon viel früher auf die Idee gekommen sind, Flyer verteilen zu lassen, und sind erstaunt über den Umsatz, den diese Werbemethode bringt. Nach einem halben Jahr ziehen Sie eine erste Bilanz und stellen fest: Die Anzahl der Flyerkunden ist von Monat zu Monat gestiegen. Gleichzeitig hat jedoch die Kundschaft ohne Flyer rapide abgenommen. Sie bemerken, dass oft nicht einmal mehr die Stammkundschaft ohne Flyer in den Laden kommt und so langsam empfinden Sie die monatlich zu zahlenden Provisionen als lästig. Sie fragen sich, ob die Aktivitäten von Herrn Müller wirklich legitim sind und auf welche Art und Weise er das Werbematerial an den Mann bringt. Deshalb beauftragen Sie einen guten Freund damit, Herrn Müller zu beschatten. Und dessen Bericht befördert geradezu Skandalöses zutage:

Sobald Sie als Chef nicht persönlich im Laden anwesend sind, verlässt Herr Müller sein vereinbartes Territorium und begibt sich in unmittelbare Nähe Ihres Geschäftes. Dort fängt er gezielt Passanten ab, die bereits in Richtung Ihres Geschäftes unterwegs sind, und drückt diesen den Flyer in die Hand. Um es etwas überspitzt zu formulieren: Ein Kunde müsste sich schon große Mühe geben, um nicht mit einem Flyer ausgestattet zu werden. Was würden Sie von dieser Geschäftspraxis halten? Würden Sie Herrn Müller weiterhin seine Provisionen auszahlen? Würden Sie weiterhin mit ihm zusammenarbeiten wollen? Wenn Sie die beiden letzten Fragen mit einem klaren „Nein" beantwortet haben, lesen Sie weiter. Wenn nicht, dann bitte erst recht!

Brand-Bidding und Ad-Hijacking verständlich erklärt

Auch wenn es kaum zu glauben ist: Der Betrug von Herrn Müller aus dem eben konstruierten Beispiel findet tagtäglich vor den virtuellen Ladentüren der großen und kleinen E-Commerce-Händler statt, dort jedoch auf einer abstrakteren Ebene und in einer weit weniger offensichtlichen Art und Weise. Auf den E-Com-

DER AUTOR

Bernd Otter ist freiberuflicher Webentwickler und Inhaber von „SEM-Scout.de", einer professionellen SEA/SEO-Analyse-Software. Davor war er zwei Jahre verantwortlich für die Bereiche SEO und SEM-Qualitätsmanagement bei der OTTO GmbH & Co. KG.

www.sem-scout.de

merce-Bereich angewendet, sieht das Flyer-Beispiel so aus:

Herr Müller ist Ihr Affiliate-Publisher. Sie als Warenverkäufer sind der Merchant. Das Territorium von Herrn Müller ist seine eigene Website. Und aus den Flyern, die ursprünglich verteilt wurden, werden Tracking-Cookies, über die Sie identifizieren können, welche Kunden von Herrn Müller geworben wurden. Sollte Ihnen einer dieser Fachbegriffe nicht geläufig sein, lesen Sie bitte zunächst den Grundlagen-Artikel zum Thema Affiliate-Marketing in dieser Ausgabe.

Ebenso wie Sie Herrn Müller im Flyer-Beispiel nur dann an Ihren Umsätzen teilhaben lassen wollen, wenn er Ihnen Kunden in den Laden bringt, die ohne seine Hilfe nicht gekommen wären, gilt dies auch für das Affiliate-Marketing: Begibt sich der Affiliate zu sehr in die Nähe Ihrer Website, sodass seine Marketingmaßnahmen keinen echten Mehrwert mehr für Sie darstellen, sollte keine Provisionierung mehr erfolgen. Wie sieht dieses „Zunahekommen" nun ganz konkret in der Praxis aus?

Um bei unserer Analogie zum Stationärhandel zu bleiben, betrachten wir die Google-Suchergebnisseiten als Einkaufspassage. Denn oftmals ist Google der Ausgangspunkt vieler virtueller Einkaufsbummel durch verschiedene Online-Kaufhäuser. Selbst diejenigen, die bereits wissen, welche Händler-Website sie als nächste besuchen wollen, tippen einfach den Namen des Händlers in den Google-Suchschlitz ein, anstatt den Domainnamen direkt in den Browser einzugeben. Es werden also fleißig Begriffe wie „amazon", „otto" oder „neckermann" als Suchbegriff eingegeben und meist wird dann direkt auf den obersten Link der Suchergebnisseite geklickt. Dies ist in den meisten Fällen eine SEM-Anzeige des entsprechenden Händlers. Und diese Stelle ist es, wo für betrügerische Affiliates der Spaß beginnt: Was wäre, wenn es einem Affiliate gelingt, sämtlichen Menschen, die auf dem eben beschriebenen Weg die Website des Händlers erreichen, einen Flyer bzw. Tracking-Cookie unterzujubeln? Richtig, der Affiliate bekommt sämtliche Einkäufe der ohnehin schon kaufwilligen Besucher vergütet!

Wie soll den Affiliates das gelingen, fragt man sich jetzt vielleicht? Schließlich gibt es ja auch so etwas wie Markenschutz bei Google Deutschland, der einem Dritten das Einbuchen von Markenbegriffen als Keywords verbietet bzw. verbieten soll!? Kein System ohne Lücken: Leider gibt es einige Schlupflöcher, die von findigen Affiliates genutzt werden, um eigene Anzeigen bei den Markenbegriffen der Merchants einzuschleusen. Wie diese Lücken im Detail ausgenutzt werden, soll an dieser Stelle gar nicht näher erläutert werden. Die Konsequenzen daraus für Shopbetreiber und Markeninhaber sind jedoch folgenschwer und werden in Abbildung 1 verdeutlicht.

Bevor gleich die Folgen aus einer Controller-Sicht näher betrachtet werden, definieren wir noch kurz die beiden Begriffe „Brand-Bidding" und „Ad-Hijacking" eindeutig und grenzen sie voneinander ab:

Brand-Bidding:

Die Verwendung fremder Markenbegriffe als Keywords im Suchmaschinenmarketing. In der Praxis wird dies nicht nur von Affiliates durchgeführt, sondern vor allem auch durch Konkurrenten, Online-Shops, Preissuchmaschinen etc.

Ad-Hijacking:

Steigerungsform des Brand-Biddings insofern, dass nicht nur die Markenbegriffe, sondern auch der Anzeigentext des Markenbesitzers 1:1 kopiert und eingesetzt wird, um letztendlich die Original-Anzeige mit der eigenen Kopie zu verdrängen.

Auswirkungen

Da sich dieser Artikel vor allem auf den Affiliate-Betrug im Suchmaschinenmarketing fokussieren soll, bleibt das Thema „Brand-Bidding" vorerst außen vor. Stattdessen betrachten wir die Konsequenzen des Ad-Hijackings aus einer Zahlenperspektive – was es die betroffenen Unternehmen kosten kann und wie es sich auf die Erfolgszahlen der beiden Kanäle Suchmaschinen- und Affiliate-Marketing auswirkt.

Wie in Abbildung 2 dargestellt wird, findet durch das Ad-Hijacking eine Um-

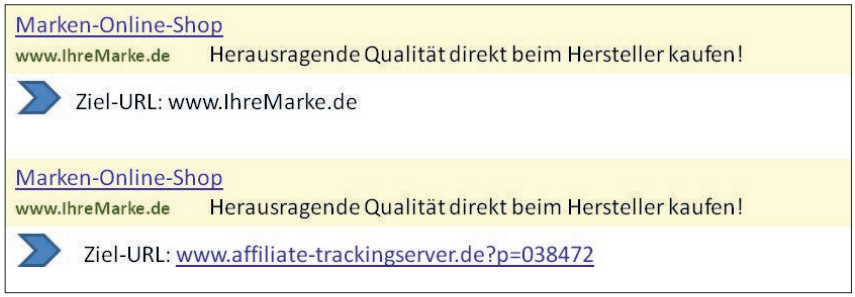

Abbildung 1 : Zweimal die gleiche Anzeige, bei der unteren jedoch wird ein Tracking-Cookie* des Affiliates gesetzt, danach erfolgt die Weiterleitung zum Markenshop. Der Surfer selbst bemerkt keinen Unterschied!

* siehe Glossar Seite 96-98

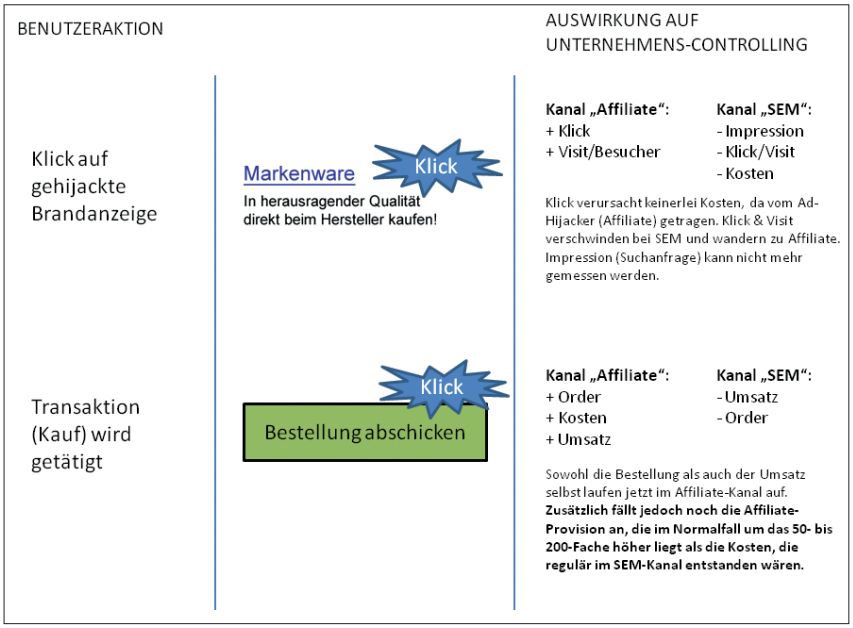

Abbildung 2: Auswirkungen des Ad-Hijacking-Betrugs auf das Controlling des betroffenen Unternehmens.

Monatliches Suchvolumen Ihrer Markenbegriffe	MONATLICHE Betrugskosten unter Annahme verschiedener Ausmaße			
	1 %	5 %	10 %	20 %
	% gehijackte Bestellungen auf Markenkeywods			
50.000	-135,- €	-675,- €	-1.350,- €	-2.700,- €
100.000	-270,- €	-1.350,- €	-2.700,- €	-5.400,- €
300.000	-810,- €	-4.050,- €	-8.100,- €	-16.200,- €
500.000	-1.350,- €	-6.750,- €	-13.500,- €	-27.000,- €
1.000.000	-2.700,- €	-13.500,- €	-27.000,- €	-54.000,- €

Für die Berechnung der Kosten wurde eine marktübliche Klickrate (CTR) von 50 % auf Brand-SEM-Anzeigen, eine Sofort-Konversionsrate von 6% sowie eine Affiliate-Provision von 9€ pro Transaktion unterstellt.

Abbildung 3: Eine Suchvolumen-/Kosten-Matrix verdeutlicht die immensen monatlichen Provisionen, die betrügerischen Affiliates aufgrund von Ad-Hijacking ausgezahlt werden.

verteilung sämtlicher Erfolgskennzahlen vom Suchmaschinenmarketing hin zum Affiliate-Bereich statt. Abgesehen von den zusätzlichen Kosten (dazu gleich mehr) geht dem Unternehmen also kein Umsatz verloren, jedoch findet höchstwahrscheinlich eine Fehlbewertung beider Marketingkanäle statt! Vor allen Dingen für Unternehmen, in denen im SEM die Kosten und Umsätze von Brand-Keywords und generischen Begriffen in einen Topf geworfen werden (die günstigen und umsatzstarken Markenkeywords also die generischen und teuren Begriffe subventionieren) ist dies von großem Nachteil. Hier braucht man sich dann über eine unbefriedigende Performance der SEM-Kampagnen nicht mehr zu wundern.

Und als ob die bislang aufgeführten Faktoren nicht schon Grund genug zur Besorgnis wären, könnte sich bei einer Einordnung des eigenen Online-Shops in die Tabelle aus Abbildung 3 durchaus ein flaues Gefühl in der Magengegend einstellen.

Betrachtet man die Summen, um die es bei Unternehmen einer gewissen Größe geht, steht außer Frage, dass es sich lohnt, einen Bruchteil des Geldes in Maßnahmen zur Erkennung dieser Betrugsfälle zu investieren. **Nicht vergessen: Die Rede ist hier von MONATLICHEN Beträgen, die unrechtmäßig an Affiliates ausgezahlt werden! Sollten den Partnern zusätzlich Post-Konversionen** (also Transaktionen, die Besucher erst bei einem späteren, erneuten Besuch der eigenen Website durchführen) **vergütet werden, liegen die Zahlen noch höher und können durchaus noch mal mit 1,5 multipliziert werden!**

Die Tricks der Ad-Hijacker

Die cleveren Betrüger bedienen sich einer Reihe von Mitteln, um unter dem Radar zu bleiben, d. h. weder durch eine unnatürlich hohe Anzahl von Sales aufzufallen noch bei einer manuellen Kontrolle des Markeninhabers entdeckt zu werden.

Geo-Targeting: Wie allgemein bekannt, hat man als Werbetreibender bei Google AdWords die Möglichkeit, seine Anzeigen nur den Nutzern in bestimmten Regionen eines Landes ausliefern zu lassen. Ad-Hijacker nutzen dies, um die Standorte des Markeninhabers und dessen SEM-Agentur aus den Kampagnen auszuschließen. Besonders eifrige Zeitgenossen buchen gar nur ein bis zwei Dutzend handverlesene Städte quer über das Land verteilt ein.

Ad-Scheduling: Zusätzlich werden die Kampagnen meist nur außerhalb der Bürozeiten des Betroffenen geschaltet, also am Abend und an Wochenenden. Dies sind die Zeiten, wo ohnehin die meisten Umsätze in Online-Shops getätigt werden und der Affiliate selbst bei einem geringen Zeitfenster der Anzeigenschaltung ein ordentliches Stück vom Kuchen abbekommt.

Referrer-Cloaking: Man sollte meinen, die über Google eingeschleusten Besucher doch eigentlich an Ihrem Referrer (ein auslesbarer Parameter, welcher die URL der zuletzt aufgerufenen Webseite enthält) erkennen und so den Affiliate dingfest machen können. Affiliates verlinken aus eben diesem Grund zunächst auf einen (oder mehrere) ihrer eigenen Server, wo der Referrer durch

Skriptsprachen verändert und durch die eigene Website-URL ausgetauscht wird. Es sieht also tatsächlich so aus, als wäre der Besucher über die Website des Affiliates zu einem gestoßen.

IP-Ausschluss: Gerade große Firmen verwenden für den Internetzugang der Mitarbeiter eine Standleitung mit eigener IP-Adresse. Sollte diese dem Affiliate bekannt sein, kann er sie gezielt ausschließen und dadurch eine Auslieferung der gehijackten Anzeigen an sämtliche PCs im Firmennetzwerk unterbinden.

Erkennungsmöglichkeiten

Die eben aufgeführten Methoden lassen es bereits vermuten: Eine manuelle Aufdeckung der Betrugsfälle ist so gut wie unmöglich. Um die schwarzen Schafe dennoch ausfindig machen zu können, bedarf es ausgefeilter Tools, welche eine automatisierte Überwachung der Markenkeywords durchführen. Wichtige Erfüllungskriterien einer solchen Software sind:

» niedrige Abfrageintervalle (um auch kurzzeitiges Hijacking zu erkennen)
» regionales Targeting
» zuverlässige Betrugserkennung, bestenfalls mit Alert-Funktionalität
» Überwachung der großen Suchmaschinen (im deutschsprachigen Raum Google, Yahoo, Bing)
» bei Unternehmen, die international tätig sind: länderübergreifendes Screening
» Nachhalten von Beweisdaten im Betrugsfall: Uhrzeit, Keywords, Screenshots, Quelltexte etc.

Es gibt mittlerweile eine Handvoll Anbieter solcher Lösungen, welche die erwähnten Kriterien mehr oder minder gut abdecken.

Wie man dagegen vorgeht

Deckt die Software einen Ad-Hijacker auf, so erhält der Kunde in der Regel direkt eine Benachrichtigungs-E-Mail, in der auch gleich die Ziel-URL des Übeltäters aufgeführt wird. Über diese URL kann letztendlich der Affiliate namentlich identifiziert werden. Denn um nachher die Hand aufhalten und eine unberechtigte Provision einfordern zu können, muss immer eine Zuordnung und damit die Identifizierung möglich sein.

Ist die Person erst einmal ausfindig gemacht, gibt es verschiedene Wege, weiter vorzugehen. Eine Stornierung der bisher getätigten (und noch nicht bestätigten) Sales sollte aber selbstverständlich sein, ebenso wie eine Abmahnung und/oder Kündigung aus dem Programm. Die Software liefert hierzu auch Beweismaterial wie die originale Google/Yahoo/Bing-Suchergebnisseite mit der gehijackten Anzeige.

Durchschnittliches Suchvolumen der Marke bei Google/Monat	Anzahl in Studie berücksichtigter Shops	Anzahl Shops mit Ad-Hijackern (im 4-Wochen-Zeitraum)	Entspricht in %
< 50.000	26	13	50 %
Bis 100.000	23	8	35 %
Bis 300.000	30	16	53 %
Bis 500.000	19	8	42 %
> 500.000	11	5	45 %
SUMME	**109**	**50**	46 %

Abbildung 4: Unterteilung der Shops nach Suchvolumen bei Google und Vorkommen von Ad-Hijacking.

SEM-Scout-Studie

Eine Studie, die im ersten Halbjahr 2010 mithilfe der Software „SEM-Scout" durchgeführt wurde, brachte einige hochinteressante Daten und Erkenntnisse. Untersucht wurden über 100 der größten deutschen Shops, die Affiliate-Programme betreiben. Hierzu wurden die wichtigsten Markenkeywords jedes einzelnen Shops automatisiert für einen Zeitraum von vier Wochen in kurzen Zeitabständen immer wieder bei allen großen Suchmaschinen abgefragt. Mit Hilfe dieser Daten wurden dann aktive Ad-Hijacker aufgespürt.

Die Ergebnisse sind alarmierend und machen deutlich, dass bei den meisten Unternehmen noch sehr viel Nachholbedarf existiert oder aber die bereits im Einsatz befindliche Software die Betrugsfälle nur unzureichend erkennt.

In Abbildung 4 werden die überwachten Marken nach ihrem Suchvolumen bei Google unterteilt dargestellt. In der dritten Spalte ist zu sehen, bei wie vielen Shops im Zeitraum der Studie mindestens ein Hijacking-Vorfall erkannt wurde. Aus der Tabelle lassen sich zwei Kernaussagen ableiten:

1. **Die Markenkeywords von fast jedem zweiten Online-Shop werden zu Betrugszwecken genutzt**
2. **Die Bekanntheit der Marke und die Größe des Shops spielen eine untergeordnete Rolle**

Um Betrügern keine unnötigen Einblicke zu geben, bleiben die genauen Methoden zur Aufdeckung solcher Betrugsfälle hier ungenannt.

Der Anteil der von Ad-Hijacking betroffenen E-Commerce-Unternehmen ist also wie erwähnt erschreckend hoch. Im nächsten Schritt ist es nun interessant zu analysieren, wie stark das Aus-

Häufigkeit, mit der das Hauptkeyword einer Marke vom Hijacking betroffen ist:	96 %

Durchschnittlicher zeitlicher Anteil, zu dem Ad-Hijacker aktiv waren:

GOOGLE	YAHOO	BING
32 % (entspricht 7,7 Std./Tag)	36 % (entspricht 8,6 Std./Tag)	41 % (entspricht 9,8 Std./Tag)

Abbildung 5: Ausmaße des Ad-Hijackings.

maß des Betrugs in diesen Fällen genau ist. In **96 % der Fälle war das Hauptkeyword betroffen**, also die wichtigste Schreibweise der Marke, so wie sie in der Regel von Suchenden eingegeben wird (Abbildung 5). **Bei 78 %** der von Hijackern heimgesuchten Shops waren **auch zusätzliche Schreibweisen wie z. B. Fehlschreibweisen oder „domain.de“ betroffen.**

Im Falle eines „Parasitenbefalls“ ist also fast immer die Originalschreibweise der Marke betroffen. Dort sind der potenzielle Umsatz für den Affiliate und zugleich der Schmerz für den Markeninhaber am größten. Allerdings werden wie festgestellt auch Falschschreibweisen etc. gerne von Hijackern eingebucht – sie werden nur wesentlich seltener gesucht und dementsprechend ist die „Freude“ daran nicht so groß. Jedoch ist auch die Gefahr, gefasst zu werden, deutlich geringer, da die meisten Firmen (wenn Sie denn bereits etwas dagegen tun) in der Regel vor allem das Hauptkeyword durch ein Tool überwachen lassen.

Weiterhin gibt die Studie Aufschluss über die Anzahl der Stunden und Tageszeiten, zu denen die Anzeigen der betroffenen Marken durchschnittlich gehijackt werden. **Bei Bing wurden Anzeigen des Markeninhabers mit durchschnittlich 9,8 Std. pro Tag durch Affiliate-Anzeigen ersetzt, was den Höchstwert darstellt. Dahinter folgt Yahoo mit 8,6 Std. und zuletzt Google mit 7,7 Std. pro Tag.** Dieses Ergebnis überrascht nicht: Das Suchaufkommen bei den kleineren Suchmaschinen ist deutlich geringer und der Hijacker muss eine längere Zeit aktiv sein, um signifikant Provisionen zu erhalten. Weiterhin liegen Yahoo und Bing nicht so sehr im Fokus der Marketingverantwortlichen, sodass die Gefahr, entdeckt zu werden, hier deutlich geringer ist. Meist schalten betrügerische Affiliates ihre Anzeigen in den Abendstunden (am Wochenende oft ausgiebiger), was der Durchschnitt von 7 bis 10 Std. pro Tag bestätigt. Abbildung 6 stellt dies anschaulich dar – die beiden Graphen aus der SEM-Scout-Software zeigen exemplarisch die Sichtbarkeit eines typischen Ad-Hijackers auf Uhrzeiten bzw. Wochentage heruntergebrochen.

Um nun das Bild des Betrugsausmaßes vervollständigen zu können, benötigt man noch Informationen über das regionale Targeting der Hijacker-Anzeigen. Wie wir nun wissen ist ein Ad-Hijacker, der ein ganzes Wochenende lang

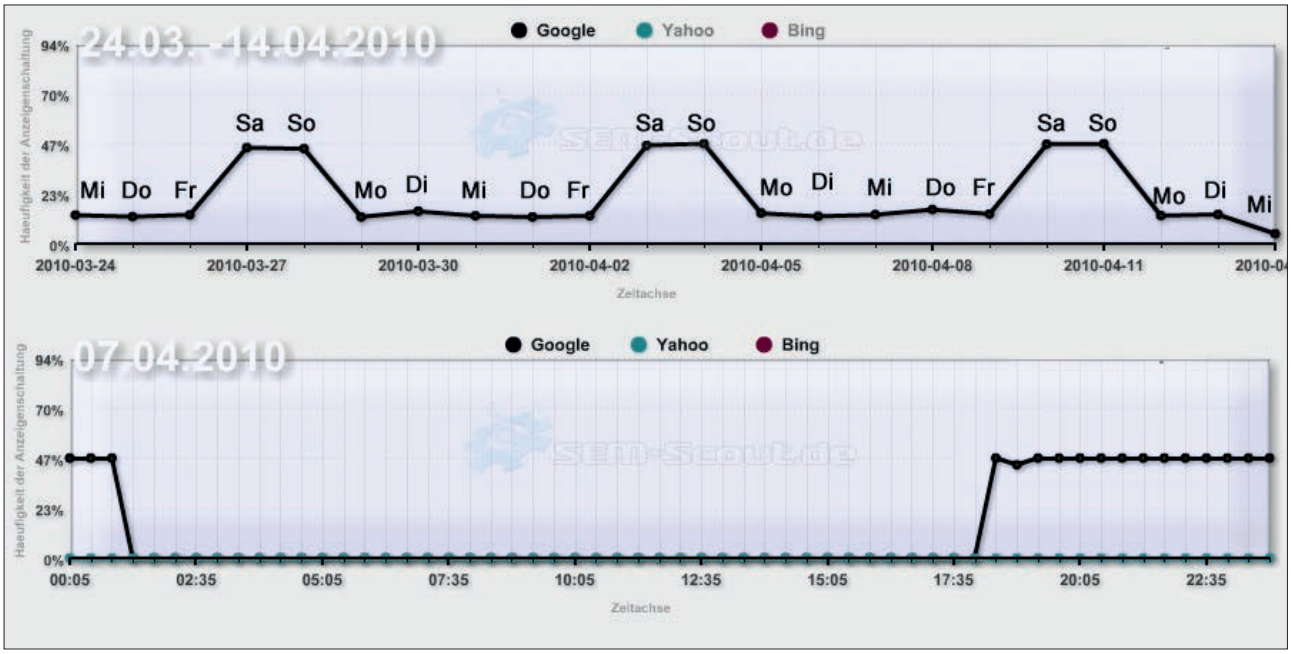

Abbildung 6: Der obere Graph zeigt die Aktivität eines Ad-Hijackers auf Wochentage bezogen, der untere betrachtet die Uhrzeiten an einem Wochentag.

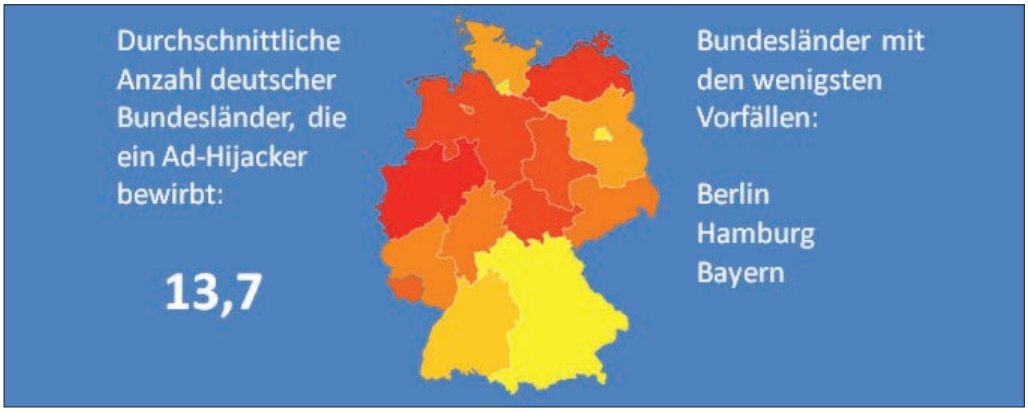

Abbildung 7: Ad-Hijacker-Heatmap für Deutschland.

Anzeigen für mehrere Keywords schaltet, meist nicht bundesweit aktiv. Wie viele Bundesländer sind es im Schnitt, in denen sie die Originalanzeige des Markeninhabers mit ihrer „Fälschung" verdrängen? Statistisch sind es 13,7 (siehe Abbildung 7). Es wird also tatsächlich meist nur der Standort des Markeninhabers und (wenn vorhanden) dessen SEM-Agentur ausgeschlossen sowie vielleicht noch ein angrenzendes Bundesland. Eine genauere Analyse zeigt, dass in Berlin mit Abstand am wenigsten „gehijackt" wurde, gefolgt von Hamburg und dem Bundesland Bayern. Das überrascht nicht, da sich hier die drei größten Ballungszentren Deutschlands befinden und dementsprechend häufig die betroffenen Firmen ansässig sind. Es macht aber auch noch mal deutlich, dass zur Entlarvung der Betrüger ein Tool notwendig ist, welches in der Lage ist, die Suchergebnisse aus sämtlichen Regionen eines Landes zu erfassen.

Fazit

Ad-Hijacking wird in Deutschland offenbar mit vielen Tricks und im großen Stil betrieben. Bei der Betrachtung der Kosten, die diese Betrugsform bei den betroffenen Unternehmen verursacht (siehe Abbildung 3), wird schnell deutlich, dass ein Teil des verfügbaren Budgets für eine Betrugserkennung sehr gut investiert scheint. Jeder Übeltäter, den man so identifizieren und ausschließen kann, spart zukünftig bares Geld. Und gegebenenfalls kommen dazu noch erfolgreich durchgesetzte, rechtliche Nachforderungen. Um die Schwere und Relevanz der durch die Studie gewonnenen Ergebnisse zu unterstreichen, hier noch einmal die wichtigsten Kennzahlen:

» Bei 50 von 109 Marken wurden während des Beobachtungszeitraums Ad-Hijacker festgestellt
» In 96 % dieser Fälle war das wichtigste, weil am häufigsten gesuchte, Markenkeyword betroffen.
» Waren Betrüger aktiv, wurde die Anzeige des angegriffenen Markeninhabers etwa 30–40 % der Zeit durch die des/der Affiliates ersetzt. Bevorzugt wurden dabei die Abendstunden und das Wochenende – Zeiten, zu denen die meisten kaufwilligen Surfer im Netz unterwegs sind.
» Die Kampagnen der Betrüger wurden den Google-Nutzern in durchschnittlich 13,7 der deutschen Bundesländer angezeigt, was den Großteil der Bevölkerung ausmacht.

Sehr vorsichtig geschätzt werden also offenbar aktuell bei den in der Studie analysierten Unternehmen etwa 15 bis 30 % der Bestellungen, die normalerweise kostengünstig über die SEM-Anzeige der Marke erwirtschaftet worden wären, sehr viel teurer in Form von unrechtmäßigen Affiliate-Provisionen bezahlt. Berücksichtig man nun noch die am 14. September in Kraft tretende Änderung der Markenrichtlinie bei Google, nach der nun auch geschützte Markenbegriffe von Dritten gebucht werden können, könnte sich die Brisanz dieses Themas noch weiter erhöhen. Tools zur Markenüberwachung müssen dafür rechtzeitig angepasst und ggf. neu justiert werden. Das Thema Markenschutz im Web wird also immer wichtiger und sollte von allen Markeninhabern und Shopbetreibern in ihrer SEM-Strategie ernsthaft berücksichtigt werden. ¶