



Klickbetrug bringt Werbebudgets in Gefahr

Auch bei Betrügern nimmt das Interesse an der Werbeform „Pay per Klick“ zu. Viele Marketers machen sich daher Sorge um den Erfolg ihrer Online-Kampagnen und befürchten, dass trotz hoher Kosten die Kunden ausbleiben.

von Frank Meltke

Waren 1995 erst 250 000 Deutsche im Web, so ist es heute mehr als die Hälfte der Bevölkerung. Parallel zum Siegeszug des Internets etablierte sich die Onlinewerbung. Neue Technologien ermöglichen es, Werbung individuell auf die Vorlieben und Bedürfnisse des Verbrauchers abzustimmen und dessen Reaktionen unmittelbar zu messen. Durch die wachsende Bedeutung von Google & Co. gehört die Vermarktung von Werbeplätzen in den Ergebnislisten der Suchanfragen neben den klassischen Onlinewerbeformen wie Linktausch und Bannerschaltungen zu den am meisten nachgefragten Marketing-Tools. Bei der Abrechnung hat sich

sowohl beim Keyword Advertising, den bei Suchmaschinen als gesponserten Links gekennzeichneten Beiträgen, als auch beim Affiliate Marketing das Pay-per-Klick-Verfahren (PPK) etabliert. Kunden schätzen dieses Marketing-Instrument als transparent und effektiv, da sie so eine genaue Rückmeldung erhalten, wie häufig ihre Werbung angesurft wurde. Für die Suchspezialisten, Anbieter von Affiliate-Programmen sowie deren Partner, die mit einer Provision beteiligt sind, ist das Verfahren unkompliziert abzurechnen und lukrativ. Alleine durch Onlinewerbung erzielte Google 2005 weltweit rund 6,06 Milliarden US-Dollar

bei einem Gesamtumsatz von 6,14 Milliarden US-Dollar. Obwohl diesem Markt in den nächsten Jahren ein Wachstum in Milliardenhöhe vorausgesagt wird, sieht sich PPK in der Branche verstärkter Kritik ausgesetzt. Denn trotz aller Vorteile hat das Abrechnungsverfahren seine Schattenseiten: Inzwischen haben auch Betrüger entdeckt, dass sich mit dem „Klick“ Geld verdienen lässt. Es gibt verschiedene Motive für Klickbetrug. Nur von marginaler Bedeutung in den Schadensstatistiken sind so genannte Internet-Hooligans, die ohne finanzielles Interesse handeln. Erheblich größeres Zerstörungspotenzial bergen

konzertierte Aktionen angeworbener Klickkolonnen. Diese agieren beispielsweise im Auftrag von Konkurrenten eines Werbetreibenden und torpedieren missliebige Anzeigenkampagnen so lange, bis diese aus der Liste der Sponsored Links verschwunden sind. Nach Angaben der „Times of India“ werden beispielsweise indische Hausfrauen und Schüler als professionelle Klicker eingesetzt. Sie steuern gezielt Websites an, die ihnen dubiose Dienstleister zuschicken. Das Wissen, wie sich mit dem falschen Klick Geld verdienen lässt, hat sich längst zu einem lukrativen Markt entwickelt. Sucht man im Internet mit den Schlüsselbegriffen „Internet“, „Geld“ und „verdienen“, findet man mehrere Millionen Seiten, von denen die meisten auf Möglichkeiten verweisen, wie sich durch mit Begriffen wie „Qualitätstest“, „Umfragenmarketing“ oder „Testaccounts“ umschriebenen Aktivitäten im Internet Geld verdienen lässt – fast immer durch eine Form des Klickbetrugs.

BETRUG HAT VIELE URHEBER

Online-Kooperationsformen wie das so genannte Affiliate Marketing sind besonders anfällig für Missbrauch. Dabei lässt ein Unternehmen seine Leistungen oder Produkte durch so genannte Affiliates, also Partner-Websites, bewerben. Diese schalten beispielsweise ein Banner, das mit der Website des Partners verbunden ist, auf ihrem eigenen Webangebot. Jedes Mal, wenn ein Internetnutzer von der Homepage des Affiliate aus die Werbeanzeige des Partners anklickt, wird eine Provision fällig. Durch das Anklicken der Werbeanzeigen auf den eigenen Seiten können betrügerische Affiliates ihre Provisionen empfindlich in die Höhe treiben.

Häufig werden zu diesem Zwecke Softwareprogramme, so genannte Klickbots, eingesetzt. Dabei handelt es sich um weitgehend automatisierte Systeme, die möglichst unauffällig Werbeklicks produzieren. Die Möglichkeiten, „synthetische“ Abfragen scriptgesteuert ablaufen zu lassen, sind sehr umfangreich. Erst im Mai 2006 entdeckte der Antivirenhersteller Panda Software ein globales Netzwerk von über 30 000 Rechnern, die mit einer Schadsoftware namens Clickbot.A

infiziert waren. Unbemerkt von den PC-Besitzern klickten sich die Computer bei jedem Internetkontakt auf vorgegebenen Seiten von Anzeige zu Anzeige.

SUCHMASCHINENBETREIBER UNTER DRUCK

Ein Praxistest des US-amerikanischen „Marketing Experiments Journal“ im Juni 2005 zeigt das immense Ausmaß des Klickbetrugs. Bis nahezu 30 Prozent der registrierten Klicks in einem der durchgeführten Testläufe hatten einen betrügerischen Hintergrund, wurden aber größtenteils nicht erkannt und daher regulär abgerechnet. Auch laut der aktuellen Statistik eines amerikanischen Klickbetrug-Indexes (Click-Fraud-Index) bewegt sich die Zahl der betrügerischen Klicks bei etwa 14 Prozent. Die Suchmaschinenanbieter befinden sich beim Thema PPK in einer misslichen Lage. Einerseits liegt es in ihrem eigenen Interesse, Missbrauch zu unterbinden, da sie sonst ihre Geschäftsgrundlage aufs Spiel setzen. Andererseits verdienen sie an jedem Klick, unabhängig davon, ob dahinter ein Interessent mit ernster Kaufabsicht oder ein Betrüger steckt. Nicht zuletzt deswegen wird diesen häufig eine geringe Motivation unterstellt, Gaunern das Handwerk zu legen. So kam es im April 2006 im US-Bundesstaat Arkansas in einer Sammelklage gegen Google wegen der „Nichtergreifung angemessener Maßnahmen zur Erkennung und Verhinderung von Klickbetrug oder sonstigen ungültigen beziehungsweise missbräuchlichen Klicks auf Onlinewerbung“ und der damit verbundenen Schädigung von Anzeigenkunden zu einem Vergleich über 90 Millionen US-Dollar. Eine Kleinigkeit, wenn man bedenkt, dass die weltweit größte Suchmaschine seit 2001 Werbeeinnahmen von 13,3 Milliarden Dollar verbuchen konnte. Auch Yahoo hat sich jüngst außergerichtlich mit seinen Klägern geeinigt und will geleistete Zahlungen an Tausende Werbekunden zurückerstatten – in der Hoffnung, nur einen geringen Teil dessen zurückzahlen zu müssen. Hier hatte das Portal von Januar 2004 bis März 2006 9,1 Milliarden Dollar eingenommen. Natürlich stellt sich die Frage, ob dem Problem Klickbetrug generell beizukommen ist oder ob es sich um eine prinzipielle

WORAN MAN KLICKBETRUG ERKENNT

Woran können Marketers Klickbetrug erkennen?

- Die Kampagne zeigt eine ungewöhnlich schlechte Konversionsrate.
- Es sind signifikante Schwankungen in der Abrechnung erkennbar.
- Die Zahl der Seitenaufrufe und die Verweildauer pro Besucher sind niedrig.
- Hoher Traffic zu ungewöhnlichen Tages- und Uhrzeiten.
- Die technische Umgebung (Betriebssystem, Browser, Provider) der Besucher ändert sich deutlich.

Welche Abwehrmaßnahmen können Marketers ergreifen?

- Kampagnentrafic und reguläres Nutzerverhalten können mit Hilfe von Web-Controlling-Tools verglichen werden.
- Beschränkungen auf wenige Affiliate-Partner, von deren Seriosität und Leistungsstärke Marketers überzeugt sind.
- Bei Verdacht auf Klickbetrug sofort das Gespräch mit dem Werbepartner suchen und gemeinsam mögliche Ursachen aufdecken.

Schwachstelle des PPK-Geschäftsmodells handelt. Google beispielsweise testet derzeit das Modell „Cost per Action“, wo Werbetreibende nur noch dann zahlen müssen, wenn nach dem getätigten Klick tatsächlich gekauft wurde.

In jedem Fall handelt es sich um ein multikausales Problem, das eine differenzierte Betrachtung erfordert. Denn nicht hinter jedem auffälligen Verhalten muss tatsächlich Betrug stecken. Zwar deuten verschiedene Indikatoren auf Missbrauch hin, jedoch werden die Methoden der Online-Ganoven immer ausgefeilter. Beispielsweise passen diese ihr Klickverhalten gängigen Tages- und Wochenprofilen an und versuchen, mit ihren Klickintervallen Zufälligkeit zu simulieren. Durch so genannte offene Proxy-Server – Dienste, die einen Zugang zum Internet herstellen – können Cyber-Kriminelle ihre Identität verbergen. Dazu kommt, dass professionelle Klickbetrüger oft aus dem Ausland heraus agieren und somit schwer zu belangen sind.

Anbieter von Web-Controlling-Tools treten mit dem Versprechen an, durch ein lückenloses Tracking des Nutzerverhaltens möglichen Betrug aufzudecken. Zu diesem Zweck ermittelt die Software beispielsweise die Geodaten und IP-Adressen von Website-Besuchern, prüft deren Verweildauer und untersucht, zu welcher Uhrzeit und mit welcher Frequenz Anzeigen aufgerufen werden. Zusammen mit weiteren Kenndaten wie Seitenauf-rufhäufigkeiten und Konversionsraten

ergibt sich so ein aussagekräftiges Bild, das Rückschlüsse zulässt, ob es sich bei einem Anwender um einen regulären Besucher oder einen Betrüger handelt. Eine Garantie, unlauteren Wettbewerb mit Hilfe solcher Programme lückenlos zu unterbinden, gibt es aber nicht.

DER RICHTIGE MIX MACHT'S

Für viele Marketers überwiegen die Vorteile, Benutzer zielgruppengenau ansprechen zu können, die Gefahren des Klickbetrugs. In jedem Fall ist es angeraten, „Pay per Klick“ mit anderen Online-Werbeformen zu kombinieren, selbst wenn dadurch Streuverluste entstehen. Neben den klassischen Onlinemarketingtools wie Bannerwerbung oder Pop-ups stehen einer Umfrage des TNS Emnid Instituts zufolge Konsumenten neuen, innovativen Werbeformen positiv gegenüber. Beispielsweise Video-Strips – entweder als kleiner Film in einem Pop-up oder platziert wie ein Banner – machen durch bewegte Bilder auf sich aufmerksam und wecken die Neugierde der User. Hohe Kosten aber keine Kunden – es gibt Alternativen. Ein gesunder Marketing-Mix aus „Pay per Klick“-Anzeigen, klassischen Onlinewerbeformen und innovativen Werbekonzepten ist eine effektive und sichere Alternative zu einer reinen Key Word Advertising-Strategie. ■

Frank Meltke ist Gründer und CEO der Contraco Consulting & Software Ltd. Kontakt: www.contraco.net