Klickbetrug und Affiliate-Hopping

Die miesen Tricks der Internet-Ganoven

Betrug im CPC-Geschäft
Betrug im Affiliate-Marketing
E-Business-Betrüger: Eine anonyme Masse
Maßnahmen gegen Betrug im E-Business

etracker®
Know Now.

Inhalt

Einleitung . . . . . S. 1

1. Betrug im CPC-Geschäft . . . . . S. 3
1.1 Klickbetrug im Keyword Advertising . . . . . S. 3
1.2 Klickbetrug bei Google AdSense . . . . . S. 4

2. Betrug im Affiliate-Marketing . . . . . S. 6

3. E-Business-Betrüger: Eine anonyme Masse S.12
3.1 Wie Betrüger ihre Spuren verwischen S.12
3.2 Häufigkeit von E-Business-Betrug S.14

4. Maßnahmen gegen Betrug im E-Business S.16
4.1 Grundsätzliche Maßnahmen gegen Klickbetrug . . . S.16
4.2 Spezielle Maßnahmen bei Affiliate-Marketing S.19

5. Fazit S.21

Die etracker GmbH aus Hamburg ist einer der führender Anbieter von Produkten und Dienstleistungen zur Optimierung von Websites und Online-Marketing-Maßnahmen.

Die etracker GmbH wurde im Jahre 2000 gegründet und ist als erstes Web-Controlling Unternehmen durch den Hamburger Datenschutzbeauftragten geprüft worden. Alle Daten werden 100 % konform zu europäischen und deutschen Datenschutzgesetzen verarbeitet.

Testen Sie alle etracker-Produkte kostenlos unter **www.etracker.com**

Zu unseren mehr als 60.000 zufriedenen Kunden zählen

Einleitung

Die Gefahr, im Internet Opfer von Diebstahl und Betrug zu werden, steht den Risiken der realen Geschäftswelt inzwischen in nichts mehr nach. Müssen sich Privatkunden mit kriminellen Auswüchsen wie Phishing, URL-Spoofing und Dialern herumschlagen, so werden Internet-Unternehmen von Klickbetrug und Affiliate-Hopping heimgesucht. Und diese beiden Ausprägungen illegaler Web-Aktivitäten richten genau da Unheil an, wo es viele Unternehmen besonders schmerzt: im Online-Marketing. Denn so effizient die unterschiedlichen Instrumente der virtuellen Absatzförderung auch sind, sie regen leider immer wieder den Einfallsreichtum der Betrüger an. Die meisten Varianten des Online-Betrugs gehen inzwischen weit über die Grenzen von vereinzelten Konkurrenzschädigungen hinaus. Betrügerische Geldmacherei ist längst keine Seltenheit mehr – und dabei geht es häufig um beträchtliche Summen. Anbieter von Suchmaschinen- Marketing und Affiliate-Plattformen wie Google, Yahoo! Search Marketing, Miva, affilinet, TradeDoubler oder zanox mussten in den vergangenen Monaten einen starken Vertrauensverlust bei ihren Kunden verzeichnen.

Die Zahl der Werbetreibenden, die gegen ihre Marketing-Partner klagen, häuft sich. Bereits 2004 zahlte Google regelmäßig einen Anteil seiner Umsätze an die Werbekunden zurück – als Ausgleich für mögliche Klickbetrügereien. Im Rahmen einer Sammelklage gegen Google wurde im Juli 2006 ein Vergleich geschlossen, der Google zur Zahlung von 90 Millionen US-Dollar an seine Kunden verpflichtet. Und auch diese beträchtliche Summe resultiert ausschließlich aus Schäden, die auf Klickbetrug zurückzuführen sind. Auf Kundenseite ist man sich einig, dass Suchmaschinen-Betreiber und Affiliate -Plattformen weitreichendere Maßnahmen ergreifen müssen, um sich und ihre Werbepartner vor der kriminellen Energie von Internet-Betrügern zu schützen. Letzten Endes stellen sich allen Beteiligten dieselben Fragen: Wie lässt sich Betrug im Internet systematisch aufdecken? Ist es vielleicht sogar möglich, kriminelle Handlungen zu verhindern? Mit welchen Mitteln können die tatsächlichen Betrüger identifiziert und darüber hinaus auch haftbar gemacht werden?

Um diesen Fragestellungen auf den Grund zu gehen, werden im Folgenden drei wesentliche Formen von Betrügereien im E-Business unterschieden: Klickbetrug im Keyword Advertising und bei Google AdSense sowie betrügerische Machenschaften im Affiliate-Marketing. Dieses Whitepaper erklärt die Wirkungsweise der einzelnen Betrugsformen anhand von Beispielen. Zudem liefert es Informationen zu den technischen Hintergründen und bietet wertvolle Hinweise, wie sich illegale Machenschaften erkennen und sogar vermeiden lassen. Dem Betrug im Affiliate-Marketing ist aufgrund seiner horrenden Ausbreitung ein eigenes Kapitel gewidmet, das die kriminellen Facetten dieser speziellen, außerordentlich raffinierten Betrugsform ans Licht bringt. Auch hier wird auf Möglichkeiten zur Unterbindung von Missbrauch und Betrug hingewiesen. Nur so können Online-Unternehmer den Internet-Ganoven das Handwerk legen.

1. Betrug im CPC-Geschäft

Drei Formen von Klickbetrug

Ein Großteil der Klickbetrügereien spielt sich rund um die Marketing-Maßnahmen ab, bei denen pro Klick abgerechnet wird. Diese spezielle Form der Online-Werbung, das Cost-per-Click oder kurz CPC-Modell, kommt sowohl im klassischen Keyword Advertising als auch beispielsweise bei Google Adsense zum Einsatz.

1.1 Klickbetrug im Keyword Advertising

Abrechnung nach CPC-Modell

Sponsored Links sind Textanzeigen in Suchmaschinen, die nach der Eingabe eines Suchbegriffs über oder neben den klassischen Ergebnissen des natürlichen Indexes einer Suchmaschine angezeigt werden. Bei den Sponsored Links, auch Keyword Advertising genannt, rechnen Suchmaschinenbetreiber nach dem CPC-Modell mit dem Werbetreibenden ab: Ähnlich einer Auktion wird die Werbung des Meistbietenden ganz oben in der Liste der käuflichen Links angezeigt.

Schädigung von Mitbewerbern durch manuelles und automatisiertes Klicken

Die simpelste Variante des Klickbetrugs im Keyword Advertising zielt auf die finanzielle Schädigung der Konkurrenz ab. Dazu klickt ein Mitbewerber meist manuell mehrfach auf den Sponsored Link seines Konkurrenten – dieser muss deshalb letztlich auch für Klicks zahlen, die nicht von seiner Zielgruppe stammen. Regelrecht professionell wird der Klickbetrug, wenn sogenannte Robots oder Click-Bots zum Einsatz kommen. Bei diesen handelt es sich um Software Tools, die automatisch und mit hoher Frequenz auf Sponsored Links und Werbeanzeigen klicken. Automatisiertes Klicken ist für Betrüger insbesondere dann ein probates Mittel, wenn die Werbeanzeige, die ein Mitbewerber geschaltet hat, komplett aus der Liste der Sponsored Links verschwinden soll. Durch ein Tagesbudget legt der Werbetreibende nämlich die maximalen Ausgaben und damit die Anzahl der möglichen Klicks pro Tag fest. Die Robots können darum einfach so lange auf einen gut gelisteten Link klicken, bis dessen festgelegte Tagessumme ausgeschöpft ist. Häufig wird so das CPC-Budget durch die Robots bereits in der Nacht aufgebraucht. Die Folge: Der Mitbewerber ist am Morgen ganz aus der Liste der Sponsored Links verschwunden, seine Anzeige erscheint an diesem Tag nicht mehr. Inzwischen bieten sogar Dritte ihre Dienste an, wenn es darum geht,

die Konkurrenz entweder durch manuelles oder durch automatisiertes Klicken auf die Sponsored Links zu schädigen.

Bei aufgebrauchtem Tagesbudget verschwindet der Konkurrent

Beispiel: Ein namhafter Anbieter von Krankenversicherungen wird bei einer Suchmaschine in den Sponsored Links an erster Stelle gelistet, sobald ein Internet-Nutzer die Suchbegriffe „Krankenversicherung Vergleich“ eingibt. Er zahlt dafür den Betrag von 7,50 Euro pro Klick; das Tagesbudget ist auf 11.250 Euro, also exakt 1.500 Klicks festgelegt. Nun beauftragt ein Konkurrenzunternehmen einen Klickbetrüger mit dem Wegklicken des Mitbewerbers. Mit einer speziell zu diesem Zweck entwickelten Robot-Software ist es für den Betrüger ein Leichtes, 1.500 Klicks zu tätigen. Er beginnt damit kurz nach Mitternacht, und am folgenden Morgen ist der Krankenversicherungsanbieter aus der Liste der Sponsored Links verschwunden. Dem Werbetreibenden ist dabei ein doppelter Schaden entstanden: Zum einen hat er mehrere tausend Euro in eine Marketing-Maßnahme investiert, die absolut keinen Nutzen erzielt, zum anderen entgehen ihm für den entsprechenden Tag Neukundengewinne, Interessenten geraten an die Konkurrenz.

1.2 Klickbetrug bei Google AdSense

Gut platzierte Werbeanzeigen auf themenspezifischen Partnerwebsites

Das AdSense-Programm von Google ist eine erweiterte Form des Keyword Advertising. Es ermöglicht dem Werbetreibenden, seine Werbeanzeige zusätzlich auf themenrelevanten Partnerwebsites zu platzieren. Um AdSense als Online-Marketing-Instrument zu nutzen, müssen Website-Inhaber beim Keyword Advertising in Google AdWords nur die Option „Google Content Network“ einschalten. Die Werbeeinblendungen erscheinen dann sowohl in Suchmaschinen in Form von Sponsored Links als auch auf inhaltlich adäquaten Websites.

Google prüft im Vorfeld all jene Websites, die sich als Werbeträger zur Verfügung stellen, auf ihre Seriosität und ihre thematische Eignung. Die Einblendung der Anzeigen erfolgt nach der Kontrolle dieser werbetragenden Websites und der Festlegung der Keywords jedoch automatisch. Auch hier wird über das CPC-Modell abgerechnet. Ein Teil der Klick-Einnahmen kommt dabei dem Inhaber der werbetragenden Seiten zugute, ein Teil geht an Google.

Betrügerische AdSense-Klicks

Die Motivation zum Klickbetrug bei Google AdSense liegt weniger in der Schädigung der Konkurrenz als schlichtweg darin, dass ein Website-Betreiber, der Google AdSense auf seiner Website schaltet, durch zahlreiche Klicks mehr Geld verdienen kann. Deshalb geht ein Großteil der Betrügereien bei Google AdSense auf das Konto von Werbepartnern, die – manuell oder automatisiert auf die Links der bei ihnen gelisteten Unternehmen klicken. Die Zahl der Betrüger, die zum Schein thematisch relevante Websites erstellen, nimmt inzwischen be- trächtliche Ausmaße an.

Gewinne durch speziell erstellte Themenportale

Beispiel: Ein Online -Händler von Trekking-Ausrüstungen definiert in Google AdWords unter anderem die Keywords „Zelten", „Camping" und „Trekking" für seine Werbeanzeigen. Gleichzeitig aktiviert er Google AdSense für die zusätzliche Werbeeinblendung auf themenspezifischen Websites. Dadurch erscheint der Link zu seinem Online-Shop jetzt automatisch beispielsweise auch auf Special-Interest-Portalen zum Thema Trekking und auf Websites von Individualreiseanbietern. Eine der Special-Interest-Seiten, ein Forum zum Thema „Camping in Skandinavien", ist ausschließlich erstellt worden, um als Werbeplattform Gewinne zu erzielen. Der Betreiber des Camping-Forums begnügt sich jedoch nicht mit den regulären Einnahmen, die er durch die Klicks seiner Website-Besucher auf die Links des Trekking-Ausrüsters erzielt. Er steigert seine Erträge dadurch, dass er mehrfach am Tag selbst auf die entsprechenden Links klickt, intelligente Robots zur Klickgenerierung einsetzt oder professionelle Klickbetrüger beauftragt. Hier entstehen für den Werbenden je nach Höhe des CPC ebenfalls erhebliche finanzielle Schäden – ganz abgesehen davon, das vielleicht seine gesamte Online-Marketing-Kampagne ohne Wirkung verpufft.

2. Betrug im Affiliate-Marketing

Erfolgsbezogene Werbepartnerschaft

Neben den professionellen Klickbetrügern, die sich durch die Manipulation von Cost-per-Click-Programmen bei Google, Yahoo! und Co. bereits bis zu 30 Prozent der eingesetzten Budgets unter den Nagel reißen, erschleichen sich sogenannte Affiliate-Hopper mit unlauteren Mitteln Provisionen und Gewinnbeteiligungen. Denn beim Affiliate-Marketing zählt in den meisten Fällen nicht die Summe der Klicks, sondern der Erfolg der einzelnen Werbemaßnahmen.

Die Vorteile des klassischen Empfehlungsmarketings nutzen

Im Affiliate-Marketing besinnen sich Internet-Händler (Merchants) auf die Vorteile des klassischen Empfehlungsmarketings aus dem Offline-Business. Wer einen größeren Kreis potenzieller Kunden auf sein Web-Angebot aufmerksam machen will, der kann als Merchant mithilfe von Affiliate-Plattformen wie affilinet, TradeDoubler oder zanox interessante Werbepartner, sogenannte Affiliate-Websites, gewinnen. Diese Websites bieten in der Regel ergänzende Produkte und Dienstleistungen zu den beworbenen Produkten an oder richten sich an eine ähnliche Zielgruppe. Der Affiliate-Partner eines Merchants, beispielsweise der Webmaster einer Website, bindet dabei einen vorgegebenen HTML-Code in seine Webseiten ein. Das können Banner mit Link zur Website des Werbetreibenden, aber auch Textbausteine oder gar umfangreiche Shop-Module sein. Da der Affiliate die Werbemittel eines Merchants veröffentlicht, wird er auch Publisher genannt. Gelangt der Besucher einer Affiliate-Website über eine Werbeanzeige beispielsweise in den Online-Shop eines Werbetreibenden, so erhält der Publisher für die erfolgreiche Vermittlung eine Vergütung. Pay-per-Click oder kurz PPC (pro Klick), Pay-per-Lead oder auch PPL (pro Interessent, Download, Abonnent etc.) und Pay-per-Sale beziehungsweise PPS (pro Verkauf) sind gängige Varianten der Partnervergütung, die je nach Gestaltung des Partnerprogramms auch häufig miteinander kombiniert werden. Höchst lukrativ ist für den Publisher die direkte Gewinnbeteiligung: Diese erfolgsbezogene Form der Werbepartnerschaft kann zwischen drei und 30 Prozent des Preises eines bestellten Produkts einbringen.

Erfolgsbezogene Werbepartnerschaft auf Provisionsbasis

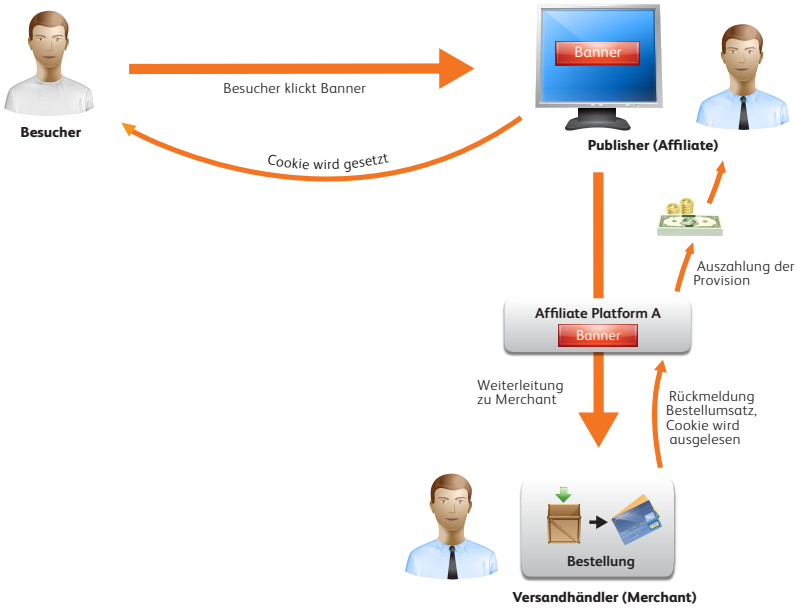
Bevor irgendeine Form von Werbepartnerschaft stattfinden kann, meldet sich der Publisher zunächst auf der Affiliate-Plattform seiner Wahl mit Adress-, Konto und inhaltlichen Daten an. Anhand dieser Angaben kann der Werbetreibende bereits im Vorfeld erkennen, ob ein Publisher thematisch zu seinen Produkten passt. Gleichzeitig veröffentlicht der Merchant sein Partnerprogramm mit Angaben zum Inhalt der Kampagne und zur Vergütung. Zudem stellt er seine Werbemittel – Banner, Pop-ups, Textbausteine usw. – auf der Affiliate-Plattform ein. Ist der Publisher an dem Programm eines Merchants interessiert, kann er sich hierzu per Knopfdruck anmelden. Daraufhin führt der Affiliate-Manager, in der Regel ein Mitarbeiter des Merchants, einen letzten redaktionellen Check der Publisher-Website durch. Sobald der Affiliate-Manager grünes Licht gibt und den Publisher annimmt, lädt dieser die Werbemittelcodes des Merchants herunter und baut sie in seine Website ein. Zwar sind sämtliche Werbemittel rein äußerlich vollkommen identisch, sie werden jedoch mittels eines speziellen Links für jeden Publisher personalisiert. Dieser Link ermöglicht es, jeden Werbemittel-Klick und einen eventuell später stattfindenden Abverkauf dem jeweiligen Publisher eindeutig zuzuordnen.

Werbesynergie durch Affiliate-Partner

Klickt nun ein Besucher der Publisher-Website auf das Banner eines Merchants, führt der Link hinter dem Werbemittel zunächst immer zur Affiliate-Plattform – der Besucher merkt davon natürlich nichts. Erst wenn die Affiliate-Plattform ein Cookie im Browser des Werbemittel-Klickers hinterlegt hat, wird der interessierte Surfer auf die Website des Online-Händlers weitergeleitet. Kommt es zu einem Kauf, wird auf der Bestellbestätigungsseite des Merchants ein HTML-Code in Form eines unsichtbaren Pixels geladen. Hierbei wird der dem Besucher beim Werbemittel-Klick gesetzte Cookie von der Affiliate-Plattform wieder ausgelesen und dieser Verkauf dem Publisher zugerechnet. Dabei ist es nicht zwingend erforderlich, dass der Kauf unmittelbar nach dem Klick auf das Werbemittel der Affiliate-Website stattfindet. Wenn es zu einem nachträglichen Kauf kommt, der sogenanntenPost-Conversion, erhält der Publisher häufig noch bis zu 30 Tage, nachdem der Käufer über dessen Website auf das entsprechende Produkt aufmerksam geworden ist, die vereinbarte Vergütung. Zudem gilt die Regel „last cookie wins“. Im Klartext bedeutet das, dass derjenige Publisher die Provision

für einen Verkaufsabschluss zugewiesen bekommt, auf dessen Website jüngst die Werbemittel des Merchants geklickt wurden.

Funktionsweise Affiliate-Marketing



Affiliate-Betrüger rechnen mehrfach ab

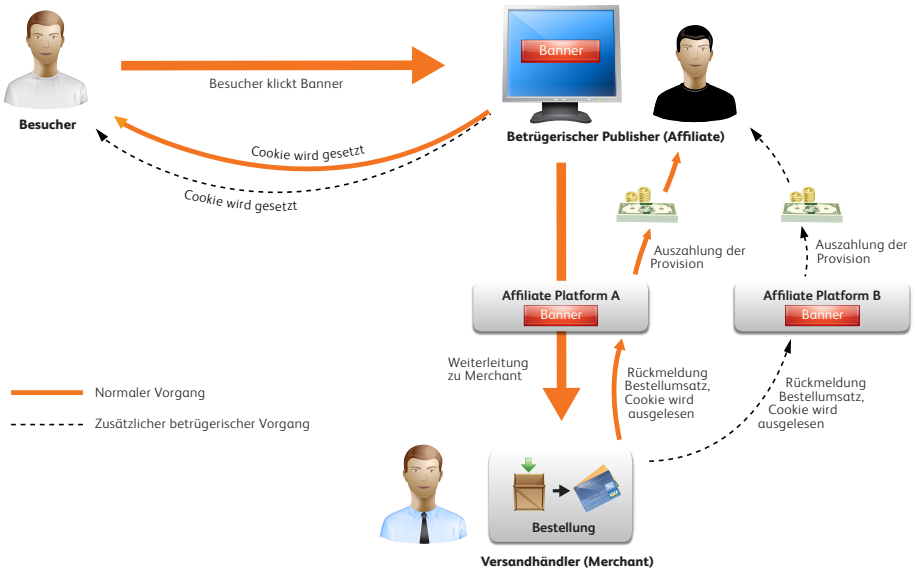
Im Affiliate-Marketing wird nur selten über Einzelklicks auf Banner oder Links betrogen, da PPC-Modelle hier keine große Verbreitung haben. Die geringen Klickpreise bieten – anders als im Keyword Advertising – keinen großen Anreiz für Betrüger. In den meisten Fällen erschleichen sich sogenannte „Affiliate-Hopper“ unrechtmäßig Provisionen, indem sie für denselben Merchant auf mehreren Affiliate-Plattformen als Publisher registriert sind. So ist es möglich, dass dem Publisher ein und derselbe Einkauf bei einem Merchant durch die unterschiedlichen Plattformen mehrfach vergütet wird. Da die einzelnen Affiliate-Plattformen autark arbeiten und einen Cookie einer anderen Plattform nicht auslesen können, ist es technisch für die Plattform-

betreiber nicht möglich, diesen Betrug festzustellen. Diese Betrugsvariante funktioniert nur dann, wenn Merchants ihr Partnerprogramm auf mehreren Affiliate-Plattformen betreiben und auf diesen dieselben Publisher an dem Programm teilnehmen.

Simples System: Mehrere Cookies für einen Werbemittelkontakt

Die technische Umsetzung von Affiliate-Hopping ist simpel: Schaltet ein Merchant im Rahmen seiner Kampagne Werbemittel auf verschiedenen Affiliate Plattformen, veröffentlicht der Publisher diese zwar auf seiner Website, er verlinkt sie jedoch so geschickt, dass der Besucher Cookies von jeder der Affiliate-Plattformen gesetzt bekommt – auch wenn er nur auf ein einziges Werbemittel klickt.
So geht bei Abschluss einer Transaktion dieses Besuchers jeweils eine Rückmeldung an die einzelnen Affiliate-Plattformen, auf denen der Merchant sein Programm betreibt, obwohl es nur einen Kaufabschluss gab.
Resultat: Der Betrüger kassiert die Provision für eine einzelne Transaktion gleich mehrfach.

Funktionsweise Affiliate-Betrug



Fehlender Rückkanal erleichtert Affiliate-Hopping

Möglich ist diese Form des Betrugs zum einen, weil es zwischen den einzelnen Affiliate-Plattformen keinen Austausch gibt. Zum anderen fallen viele Betrügereien auch deshalb nicht auf, weil der Rückkanal zwischen Online-Verkauf und Warenwirtschaft des Merchants praktisch nicht vorhanden ist. Falls ein Händler überhaupt registriert, dass die Zahl der von ihm ausgeschütteten Provisionen weit über der Zahl der Verkaufsabschlüsse liegt, ist es meist viel zu spät, um gezielt auf den Betrug zu reagieren und einzelne Betrüger in der Masse der seriösen Publisher ausfindig zu machen. Dieser mangelhafte Rückkanal führt des Weiteren dazu, dass häufig selbst dann eine Provision ausgeschüttet wird, wenn der Käufer die Bestellung später storniert und faktisch gar kein Kauf stattfindet. Diese Käufe mit Stornierung werden häufig von Affiliate-Betrügern selbst getätigt oder an Dritte in Auftrag gegeben. Ähnlich wie beim Klickbetrug ist es auch hier üblich, dass ein Betrüger eine Website lediglich aus dem Grund erstellt, um an Affiliate-Programmen teilnehmen und möglichst viel Provision einstreichen zu können. Betrüger schädigen damit auch ehrliche Online-Werbepartner: Denn üblicherweise bereinigt der Merchant seine Ausfälle um eine Stornoquote, die durch die betrügerischen Stornierungen der Affiliate-Hopper künstlich in die Höhe getrieben wird. Aufrichtige Publisher erhalten dadurch niedrigere Provisionen als ihnen eigentlich zustehen würden.

Geschickte Verlinkung der Werbemittel

Beispiel: Ein großes Modehaus möchte die Besucheranzahl und damit gleich zeitig die Verkaufsrate in seinem Online-Shop erhöhen. Dazu betreibt es sowohl bei affilinet und TradeDoubler als auch bei zanox ein Affiliate-Programm. Nun erstellt ein Webmaster ein Webportal zum Thema „Mode und Lifestyle“ und meldet sich bei den drei Plattformen als Publisher für das Modehaus an. Er schaltet das aktuelle Werbemittel des Modehauses jedoch nur einmal und verknüpft dieses so geschickt mit den einzelnen Programmen der Plattformen, dass ein Werbemittelklick bei allen drei Plattformen registriert wird. Nun wird nicht nur ein Cookie gesetzt, wenn ein Besucher seiner Website über das Werbemittel in den Online-Shop des Modehändlers gelangt, vielmehr sind es gleich drei. Bestellt der Kunde jetzt ein Produkt, so wird bei Bestellung ebenfalls für jede der drei Plattformen je ein unsichtbares Pixel geladen. Die Folge: Jede Plattform registriert die Bestellung und ordnet

den Verkauf dem betrügerischen Publisher zu. Der Betrüger streicht so für nur eine Bestellung dreifach die vereinbarte Gewinnbeteiligung ein.

Provision auch bei stornierter Bestellung

Doch damit nicht genug: Um seine unrechtmäßigen Erträge weiter zu erhöhen, macht sich der Affiliate-Betrüger den fehlenden Rückkanal zwischen Warenwirtschaft und Affiliate-Plattform zu Nutze. Hierzu bestellt er zunächst sehr kostspielige Produkte selbst, beispielsweise teure Herrenanzüge und Abendkleider. Diese Bestellungen storniert er jedoch umgehend. In Ermangelung einer Schnittstelle zwischen der Warenwirtschaft, in der die Stornierungen verwaltet werden, und den Affiliate-Plattformen, die den Verkauf registriert haben, ist keine Transparenz darüber gegeben, ob eine Bestellung widerrufen wurde. So kann das Modehaus im Affiliate-System nicht detailliert erkennen, welche Waren tatsächlich gekauft und welche Bestellungen storniert wurden. Der Affiliate-Betrüger nutzt diesen blinden Fleck und streicht lukrative Provisionen für Verkäufe ein, die faktisch nicht zu Stande gekommen sind. Weil ein Rückkanal zur Stornomeldung an die Affiliate-Plattform nicht vorhanden ist, nimmt das Modehaus jeden Monat eine pauschale Provisionsbereinigung vor, die sich an der aktuellen Stornoquote bemisst. Die Abzüge, die durch diese Provisionsbereinigung entstehen, sind für den Affiliate-Hopper jedoch praktisch irrelevant, denn er fährt nach wie vor enorme Provisionssummen ein – und das bei geringstem Aufwand.

3. E-Business-Betrüger: Eine anonyme Masse

Betrüger, die sich in der Unterwelt des Online-Marketings besonders wohlfühlen, zeichnen sich durch zwei ganz spezielle Merkmale aus: Zum einen verstehen sie es, sich weitestgehend unerkannt im Internet zu bewegen. Zum anderen spiegeln sie die komplette Palette kriminellen Potenzials – vom kleinen Ganoven bis hin zum organisierten Verbrecher – wider. Was aber wirklich alarmierend ist: Die geschätzte Dunkelziffer über Häufigkeit und Ausmaß von E-Business-Betrügereien wächst von Jahr zu Jahr dramatisch.

3.1 Betrüger ihre Spuren verwischen

Hinter offenen Proxies anonym im Internet surfen

Egal ob Klickbetrug oder Affiliate-Hopping, die wenigsten Internet-Gauner gehen so ungeschickt ans Werk, dass sie über ihre IP-Adresse oder Cookies ausfindig gemacht werden können. Hinter dieser kleinen Gruppe von Amateur-Betrügern verbergen sich in den meisten Fällen vermutlich Unternehmer, die durch manuelle Klicks auf Sponsored Links oder Werbebanner ihrem Konkurrenten auf die Schnelle Schaden zufügen wollen. Der Großteil der professionellen Klickbetrüger bedient sich jedoch wesentlich ausgereifterer Methoden, um über das Internet unrechtmäßig Gewinn zu machen.

Unsichtbar durch Anonymisierungstools

Inzwischen ist es selbst für Laien kein Problem mehr, sich im Internet völlig anonym zu bewegen. Viele Maßnahmen schützen jedoch nicht nur die Privatsphäre von aufrichtigen Nutzern, sie ermöglichen es auch E-Business-Betrügern, nahezu unentdeckt zu bleiben. Üblicherweise kann über die IP-Adresse, die an jeden Internet-Nutzer vergeben wird, spätestens durch einen richterlichen Beschluss festgestellt werden, wer sich hinter dem Besucher einer Website verbirgt. Das lässt sich jedoch leicht umgehen: Durch sogenannte Proxies ist es so gut wie unmöglich, einen Nutzer zu identifizieren. Proxy heißt „Stellvertreter“ und bezeichnet einen Netzwerkserver, der anstelle eines Client-Rechners Netzwerkverbindungen aufbaut und so die Rolle des Internet-Nutzers übernimmt. Ähnlich einem Boten führt der Proxy die Anweisungen des Internet-Nutzers stellvertretend für diesen durch und verwendet dabei eine eigene IP-

Adresse. Durch dieses Proxy-Prinzip kann eine Zwischenspeicherung der transportierten Daten (Caching-Proxy) und eine Datenflusskontrolle (Security-Proxy) realisiert werden. Proxy-Server werden überwiegend von größeren Unternehmen, Institutionen und Providern eingerichtet, bei denen ein reger Datenverkehr herrscht. Bei offenen Proxies handelt es sich zumeist um Server, die fehlerhaft konfiguriert sind. Sie nehmen im Gegensatz zu regulär eingestellten Proxy-Servern jegliche externe Anfrage entgegen und reichen diese in ihrem Namen weiter. So wird die Identität der anfragenden Person nicht sichtbar, letztlich kann jedermann einen offenen Proxy als virtuelle Zwischenstation verwenden. Um sich im Internet anonym hinter offenen Proxies zu bewegen, kann ein Nutzer Listen abonnieren, die entsprechende offene Proxy-Server aufführen. Wer die hierzu erforderlichen Einstellungen nicht manuell tätigen will, kann für geringe Beträge (ab 15 Euro im Fachhandel oder als Download) Anonymisierungssoftware herunterladen, die sämtliche Arbeitsschritte automatisiert. Viele Anonymisierungsinstrumente nutzen offene Proxies, um in kurzen Zeitabständen die IP-Adresse zu wechseln, mit der ein Nutzer sich im Internet bewegt. Auf diesem Weg bleiben Internet-Betrüger, die auf einzelne Links klicken, in der Regel völlig unentdeckt. Und auch die vorgetäuschte Bestellung von Produkten eines Affiliate-Merchants bleibt so anonym. Erschwerend kommt hinzu, dass viele professionelle Betrüger ausländische Proxies nutzen oder direkt aus dem Ausland heraus agieren. Sie können also selbst dann häufig nicht rechtlich belangt werden, wenn ihre Identität aufgedeckt wurde.

3.2 Häufigkeit von E-Business-Betrug

Google besorgt über wachsenden Klickbetrug

Der Betrug über den Verbrauch des Tagesbudgets (Klickbetrug im Keyword Advertising) ist in Europa zurzeit noch nicht so stark verbreitet; in den USA ist er aber längst ein großes Thema. Klickbetrug über Google AdSense bewegt sich inzwischen auch in Europa in manchen Branchen deutlich im zweistelligen Prozentbereich. Ebenso wächst die Zahl der Affiliate-Hopper. Bei großen Unternehmen, die ihre Online-Marketingaktionen über mehrere Affiliate-Plattformen gleichzeitig laufen lassen, können in Deutschland schon jetzt bis zu 20 Prozent der Provisionen auf betrügerische Maßnahmen zurückgeführt werden.

Größenordnung von Klickbetrug durch Suchmaschinen nur schwer messbar

Auf einer Aktionärsversammlung im Dezember 2004 äußerte sich Google erstmalig offiziell zum Problemthema Klickbetrug. Der Google Finanzvorstand, CFO George Reyes, zeigte sich besorgt über die aktuellen Entwicklungen und beschrieb Klickbetrug als größte Bedrohung für die Internet-Wirtschaft und das Geschäftsmodell von Google: „Ich denke, wir müssen sehr, sehr schnell etwas dagegen tun“, so Reyes*. Experten schätzen den Anteil betrügerischer Klicks im Online-Marketing inzwischen auf mehr als 20 Prozent. Anbieter von CPC- Abrechnungsmodellen wie Google, Yahoo! Search Marketing und Miva sehen dagegen den Klickbetrug in Deutschland und Europa im zu vernachlässigenden Promille-Bereich. Diese Aussage wird durch eigene Messungen der Betreiber unterstrichen. Jedoch sind die CPC-Anbieter technisch nicht in der Lage, die wirkliche Größenordnung zu messen. Den Anbietern stehen in der Regel nur Daten über den Besucher zur Verfügung, die bei der Einblendung der Werbeanzeige und beim Klick erfasst wurden. Ob der Besucher jemals die Website des Werbetreibenden erreicht und sich auf dieser wie ein regulärer Nutzer verhält, bleibt ihnen verschlossen.

* Zitat im Original: „Click fraud is the biggest threat to the Internet economy. There's a lot of bad guys out there that are trying to take advantage of this and it costs, I'm sure not just us, but eBay, and Yahoo! and Amazon and the whole crowd, you know, tons of money. I think something has to be done about this really, really quickly, because I think, potentially, it threatens our business model."

Quelle: CNN Money http://money.cnn.com/2004/12/02/technology/google_fraud/

Das wirksamste Mittel, um Betrügereien im Internet-Handel zu erkennen, ist ein durchgänges Tracking des Besucherverhaltens.

4. Maßnahmen gegen Betrug im E-Business

4.1 Grundsätzliche Maßnahmen

Einmessen der Website als Maßnahme gegen Klickbetrug

Das wirksamste Mittel, um Betrügereien im Internet-Handel zu erkennen, ist ein durchgängiges Tracking des Besucherverhaltens. Kennt ein Online-Verantwortlicher das natürliche Verhalten auf seiner Website, so kann er Abweichungen im Nutzerverhalten, die auf Klickbetrug hinweisen, schnell erkennen. Um eine Website und ihr natürliches Verhalten zu messen, empfiehlt es sich, zunächst nur jene Nutzer zu beobachten, die nicht über Affiliate-Maßnahmen oder Sponsored Links auf die Website gelangen. Bei dieser Messung werden im regulären Website-Traffic unter anderem folgende Kennzahlen betrachtet:

- **Geografie:** Aus welchen Ländern, Regionen und Städten kommen die Besucher?
- **IP-Adressen:** Haben die Besucher Proxies genutzt? Wurde ein Großteil der Werbemittelklicks und Abverkäufe von offenen Proxies aus getätigt?
- **Technische Daten:** Welche Betriebssysteme, Browser, Provider etc. verwenden die Besucher?
- **Verweildauer:** Wie lange haben sich die Besucher auf der Website aufgehalten?
- **Seitenaufrufhäufigkeiten:** Wie viele/welche Seiten wurden aufgerufen?
- **Zeitverhalten:** Zu welcher Uhrzeit und mit welcher Frequenz wird auf Anzeigen geklickt?
- **Konversionsraten:** Wie viele Käufe oder Transaktionen

wurden korrelierend zur entsprechenden Werbemaßnahme getätigt?

- **Werbemittelkontakte:** Mit welchem Werbemittel hatte der Besucher den letzten und damit zu wertenden Werbemittelkontakt?

Abweichungen vom natürlichen Verhalten deuten auf Klickbetrug

Nachdem die Website und ihr natürlicher Traffic analysiert und eingemessen sind, startet das übergreifende Web-Controlling, in das sämtliche Besucher der Website einbezogen werden. Also auch diejenigen, die über CPC-Modelle und Affiliate-Kampagnen auf die Website gelangt sind. Weichen nun einer oder mehrere der Parameter erheblich von den zuvor analysierten Mustern ab, ist es mehr als wahrscheinlich, dass der Werbetreibende Klickbetrügern zum Opfer gefallen ist. Wann genau die Indizien auf einen Klickbetrug hinweisen, hängt von den spezifischen Kriterien einzelner Website-Inhaber ab. So können zum Beispiel vermehrte Klicks zu einer unüblichen Uhrzeit oder eine große Zahl von Seitenaufrufen aus dem Ausland Hinweise auf betrügerische Aktivitäten sein.

Keine Chance für intelligente Klick-Programme

Gerade bei Click-Bots, über die betrügerisches Klicken automatisch abgewickelt werden kann, werden Abweichungen vom Verhalten realer Website-Besucher schnell deutlich. Besonders auffällig sind in diesem Fall beispielsweise Seitenzugriffe, bei denen der mutmaßliche Besucher nach dem Aufruf der Startseite die Website direkt wieder verlässt. Häuft sich ein derartiges Verhalten, liegt auch hier wieder der Betrugsverdacht nahe. Selbst bei intelligenteren Click-Robots, die sich dem menschlichen Verhalten entsprechend mit mehreren Klicks über eine Website bewegen, lassen sich mit einem übergreifenden Web-Controlling auf kurz oder lang Abweichungen vom natürlichen Traffic feststellen.

IP-Adressen von offenen Proxies erhärten Verdacht

Ein spezieller Indikator für systematischen Klickbetrug ist das verstärkte Aufkommen von IP-Adressen, hinter denen sich offene Proxies verbergen. Um auf Klickbetrüger aufmerksam zu werden, die sich auf diese Weise anonymisieren, abonnieren die Suchmaschinen-Betreiber Listen offener Proxies und gleichen diese mit den bei Werbemittel-Klicks gemessenen IP-Adressen ab. Decken sich die IP-Adressen der Liste mit denen verdächtiger Werbemittel-Klicks, kann es vorkommen, dass der Betreiber die entsprechenden Vergütungen im Verdachtsfall nicht ausschüttet und dem Werbetreibenden automatisch rückerstattet bzw. nicht berechnet. In der Regel ist heute jedoch immer noch der Website-Betreiber gefordert, die abgerechneten Klicks mit einem weiteren Web-Controlling System zu überprüfen und Verdachtsfälle zwecks Rückerstattung an den Werbepartner zu melden.

etracker Kampagnenreport inkl. Klickbetrugsanalyse

4.2 Spezielle Maßnahmen im Affiliate-Marketing

Hauseigene Tracking-Anwendungen sind häufig nicht rentabel

Um Affiliate-Hopping zu verhindern, können Online-Händler selbst ein aufwändiges Cookie-Tracking auf ihrer Website implementieren. Mithilfe dieses Trackings muss der Merchant genau erkennen, von welcher Affiliate-Plattform einzelne Kunden auf seine Website kommen und welche Plattform tatsächlich den letzten Werbemittelkontakt herbeigeführt hat. Auf der Basis dieser Information wird dann sichergestellt, dass bei Abschluss einer Transaktion die Transaktionsbestätigung nur an die Plattform gesendet wird, über die der jüngste Werbemittelkontakt zustande kam. Die Krux dieser Lösung: Für den Merchant ist der Aufwand, eine derartige Tracking-Applikation zu entwickeln und zu betreiben, mit erheblichen Kosten verbunden und häufig nur mit externem Know-how zu bewältigen. Daher ist der Einsatz einer intelligenten Web-Controlling Lösung, die Affiliate-Betrüger aktiv abwehrt, in den meisten Fällen die wesentlich kostenfreundlichere Alternative.

Übergreifende Kontrolle durch Pixel-Technologie

Beim Affiliate-Betrug ist eine Form des Web-Controlling besonders wirkungsvoll: Mittels Pixel-Technologie lässt sich exakt feststellen, welcher Käufer über welche Affiliate-Website in einen Online-Shop gelangt ist. Durch solch in übergreifendes Web-Controlling lassen sich Affiliate-Maßnahmen unabhängig von den erhobenen Daten der Affiliate-Plattformen kontrollieren. Im Gegensatz zu den Plattform-Betreibern, die Werbemaßnahmen lediglich im unmittelbaren Zusammenhang mit ihrem Affiliate-System überprüfen, erfasst ein übergeordnetes Web-Controlling den Traffic einer Website in einem wesentlich weitreichenderen Kontext. So können durch die Pixel-Technologie mehrfache Provisionsausschüttungen von vornherein vermieden werden, denn der letzte Kontakt mit der Werbemaßnahme und die tatsächliche Konversion erscheinen in ihrem unmittelbaren Zusammenhang. Der Shop-Betreiber sieht hier den tatsächlichen Abverkauf nur einmal, weil nicht mehrere Pixel statisch in das Bestellbestä tigungsformular eingebunden sind, sondern dynamisch das Pixel der Plattform mit dem letzten Kontakt eingeblendet wird.

Nach Möglichkeit nur eine Affiliate-Plattform

Vom Betrug durch Affiliate-Hopper sind besonders große Unternehmen betroffen, die aufgrund ihrer umfangreichen Marketing-Maßnahmen die Affiliate-Programme auf mehreren Plattformen parallel betreiben. Unternehmen, deren Marketing-Erfolg nicht zwingend davon abhängt, dass sie auf mehrere Plattformen zurückgreifen, sollten sich ausschließlich auf ein Affiliate-Programm beschränken. Diese Maßnahme bietet als einzige eine 100-prozentige Sicherheit gegen Betrug durch Affiliate-Hopper.

5. Fazit

Was wirklich hilft: Web-Controlling

Viele Klicks, keine Kunden, hohe Kosten – Klickbetrüger und Affiliate-Hopper verderben inzwischen vielen Werbetreibenden die Freude am Online-Marketing. Dabei sind die Instrumente der Internet-Werbung die ideale Basis für preiswerte und höchst effektive Marketing-Kampagnen. Gerade deshalb sind die Forderungen der Werbenden nach verstärkten Kontrollen und transparenteren Abrechnungsmodellen durch die Suchmaschinen-Betreiber und Affiliate-Plattformen mehr als verständlich. Wenn es auch grundsätzlich sehr schwer ist, die verschiedenen Varianten des Klickbetrugs aufzudecken, eines gilt für alle betroffenen Parteien: Ohne ein übergreifendes Web-Controlling ist es schlicht unmöglich, dem Betrug im E-Business beizukommen. Wer sich vor illegalen Machenschaften im Internet-Handel schützen und Betrüger dingfest machen will, braucht Web-Controlling.

etracker GmbH
Alsterdorfer Straße 2a
22299 Hamburg
Germany

t +49 40 55 56 59 50
f +49 40 55 56 59 59
e info@etracker.com
i www.etracker.com