

Click-Spamming:

Gefahr für Affiliate-Marketing und Partnerprogramme?

Beim „Click Spamming“ ruft eine Person eine Online-Werbeanzeige mittels eines automatisierten Skriptes auf und verursacht so bewusst hohe Zugriffszahlen. Bei dieser neuen Form des Missbrauchs sind sämtliche Verfahren betroffen, die click-basiert abrechnen. Bekanntes Beispiel hierfür sind die Google AdWords, jedoch auch sämtliche Partner-Programme, die via Pay-per-Click abrechnen. Ein Überblick.

Von Dr. Martin Bahr

1. Das Phänomen: „Click Spamming“

In der letzten Zeit taucht in regelmäßigen Abständen immer wieder der Begriff „Click Spamming“ auf, vgl. z.B. den Bericht von Bager in der c't 13/2004, S. 170. Beim „Click Spamming“ ruft eine Person eine Online-Werbeanzeige mittels eines automatisierten Skriptes auf und verursacht so bewusst hohe Zugriffszahlen. Bei dieser neuen Form des Missbrauchs sind sämtliche Verfahren betroffen, die click-basiert abrechnen. Bekanntes Beispiel hierfür sind die Google AdWords, jedoch auch sämtliche Partner-Programme, die via Pay-per-Click abrechnen, vgl. zu Letzterem unsere Webseite <http://www.AffiliateundRecht.de>.

Das dahinter stehende Prinzip existiert schon seit längerem im Netz und wird auch in artverwandten Konstellationen genutzt: Bei DDoS-Attacken (Distributed Denial of Service) wird einfach der betreffende Server mit derartig vielen Anfragen überhäuft, dass er diese Kapazitäten nicht mehr bewältigen kann und abstürzt. Es sind drei unterschiedliche Konstellationen denkbar, in denen „Click Spamming“ betrieben wird:

a) 1. Konstellation:

Der Affiliate erhält vom Merchant für click-basierte Leistungen (z.B. Werbeeinblendungen à la Google AdSense) eine Vergütung. Mittels automatisiertem Skript erhöht der Affiliate die Click-Zahlen.

b) 2. Konstellation:

Ein Unternehmen ruft automatisiert Online-Anzeigen eines Konkurrenten (z.B. Werbeeinblendungen à la Google AdWords) so oft ab bis dessen Tageskontingent erschöpft ist, um auf diese Weise die eigenen Anzeigen besser zu platzieren. Die Online-Anzeigen des Konkurrenten tauchen dadurch faktisch gar nicht mehr auf.

c) 3. Konstellation:

Ein Affiliate versucht, die click-basierten Online-Anzeigen auf einer speziellen Webseite eines Konkurrenten (z.B. Werbeeinblendungen à la Google AdSense) automatisiert bewusst in die Höhe zu treiben, so dass der Merchant aufgrund des offensichtlichen Missbrauchs den Konkurrenten von diesem Verfahren ausschließt. Der Konkurrent erleidet dadurch erhebliche Verluste bei den Werbeeinnahmen.

2. Das Problem: Nur begrenzte Herausgabe von Personendaten

Das Problem, das nun auftritt, ist das wie bei fast allen Internet-Delikten übliche: Damit der Merchant oder der betroffene Dritte seinen Anspruch auf Unterlassung oder Scha-

densersatz überhaupt durchsetzen kann, muss er die Identität des Schädigers kennen. Und die lässt sich im Regelfall nur anhand der IP-Nummer i.V.m. mit dem Log-File des jeweiligen Internet-Service-Providers (ISP) feststellen.

Der ISP darf diese Daten jedoch grundsätzlich nur zu Zwecken der Strafverfolgung an die Polizei, die Staatsanwaltschaft oder das Gericht weitergeben (§ 6 Abs.5 S.5 TDDSG). Das Geltendmachen von rein zivilrechtlichen Ansprüchen reicht demnach nicht aus, sondern es muss vielmehr der Verdacht einer Straftat vorliegen. Liegt nämlich eine Straftat vor, kann der Betroffene über seinen Rechtsanwalt Einsicht in die Ermittlungsakten der Strafverfolgungsbehörden nehmen und erhält auf diesem Umweg die Identität der Schädigers.

Dies bedeutet aber auch, dass wenn keine Straftat vorliegt, kaum eine Möglichkeit zur Identitätsermittlung besteht, da der ISP wegen der klaren Regelung in § 6 Abs.5 S.5 TDDSG sich weigern wird, entsprechende Daten herauszugeben.

3. Juristische Bewertung

a) 1. Konstellation:

Der Affiliate begeht hier gegenüber dem Merchant eine betrügerische Handlung, da er vorspiegelt, interessierte Dritte hätten die Online-Werbeanzeigen angeklickt.

Da die Vorspiegelung falscher Tatsachen nicht gegenüber einem Menschen, sondern einem elektronischen Abrechnungssystem erfolgt, scheidet Betrug (§ 263 StGB) aus. Jedoch ist in jedem Fall die Straftat des Computerbetruges § 263a StGB gegeben.

Somit wird die Staatsanwaltschaft ein entsprechendes Ermittlungsverfahren einleiten und der Geschädigte kann Akteneinsicht beantragen, um die Daten des Täters zu erhalten.

b) 2. Konstellation:

Problematischer ist dagegen die 2. Konstellation.

Aus dem gleichen Grunde wie oben scheidet zunächst Betrug (§ 263 StGB) aus.

Aber auch Computerbetrug (§ 263a StGB) ist hier nicht gegeben, da das Unternehmen lediglich in der Absicht handelt, den Konkurrenten zu schädigen. Es erlangt durch sein Handeln im rechtlichen Sinne auch keinen unmittelbaren Vermögensvorteil. Zwar hat das Unternehmen so einen unliebsamen Konkurrenten ausgeschaltet, aber zwischen dem Vermögensschaden auf Seiten des Konkurrenten und dem erlangten Vorteil liegt keine Stoffgleichheit vor, was § 263a StGB aber verlangt.

Auch gilt es hier zu beachten, dass der Getäuschte nicht unmittelbar die Konkurrenz, sondern das die Werbeeinblen-

Fortsetzung von Seite 11

dungen vornehmende Unternehmen (also z.B. Google) ist. Somit handelt es sich hier um einen so genannten Dreiecks-Betrug, da Getäuschter (z.B. Google) und Geschädigter (Konkurrenz-Unternehmen) nicht identisch sind. Ein solcher Dreiecks-Betrug ist aber nur dann strafbar, wenn zwischen Getäuschtem und Geschädigtem ein gewisses Näheverhältnis besteht. Nach allgemeiner Meinung reicht hierfür ein bloßes vertragliches Verhältnis wie in der 2. Konstellation nicht aus, so dass auch aus diesem Grunde § 263a StGB ausscheidet.

Eine Strafbarkeit wegen Datenveränderung (§ 303a StGB) oder Computersabotage (§ 303b StGB) kommt nicht in Betracht, da hier keine Daten verändert, sondern lediglich falsche Daten aufgezeichnet werden.

c) 3. Konstellation:

Das gleiche rechtliche Ergebnis wie bei der 2. Konstellation. Hier ist noch deutlicher, dass keine Bereicherungsabsicht beim Affiliate vorliegt, sondern einzig und allein die Absicht, die Konkurrenz zu schädigen.

4. Ergebnis

Eine strafbare Handlung ist somit nur bei der 1. Konstellation erkennbar. D.h., nur hier wird der Geschädigte über den Umweg der Akteneinsicht in die strafrechtlichen Ermittlungsakten die Anonymität des Schädigers herausbekommen. In allen anderen Konstellationen ist es dem Geschädigten nicht möglich, den Täter zu identifizieren.

Das Ergebnis ist ein ernüchterndes, zeigt aber umso mehr die dringende Notwendigkeit, dass auf Seiten des Werbeeinblendenden vornehmenden Unternehmens alle technischen Kontroll-Möglichkeiten eingesetzt werden müssen, um derartige Missbräuche zu verhindern.

Zivilrechtlich ist dagegen die Situation absolut klar. „Click Spamming“ ist zum einen eine wettbewerbswidrige Handlung (§ 1 UWG), da hier gezielt ein konkreter Wettbewerber in unsachlicher Weise geschädigt wird. Zum anderen handelt es sich um eine vorsätzliche sittenwidrige Schädigung (§ 826 BGB). Der Geschädigte hat einen Anspruch auf Unterlassung, Schadensersatz und Auskunft.

Noch eine kleine Anmerkung zuletzt:

Wer nun glaubt, sich mittels der 2. und 3. Konstellation wild austoben zu müssen, weil er ja in jedem Fall straflos ausgeht bzw. anonym bleibt, der sollte beachten, dass es durchaus ausnahmsweise vorkommen kann, dass ein ISP entgegen den gesetzlichen Bestimmungen die Daten weitergibt. Ob hier dann ein Beweisverwertungsverbot eintritt, ist bislang ungeklärt (zumal hier ein Zivilverfahren und kein Strafverfahren vorliegt).

Oben genannte TDDSG-Vorschriften sind ohnehin auf das Gebiet der Bundesrepublik Deutschland begrenzt, d.h., sie gelten nicht für ausländische ISP. Ein ausländischer ISP kann somit, soweit er nicht durch sein Heimatrecht dadurch gehindert ist, die Daten unproblematisch herausgeben.

Des Weiteren herrscht im Online-Recht in vielfacher Hinsicht eine erhebliche Rechtsunklarheit. Es kann daher durchaus sein, dass der ermittelnde Staatsanwalt bei seiner rechtlichen Würdigung der 2. und 3. Konstellation zu einem anderen Ergebnis kommt und somit, wenn auch wenig überzeugend, von einer strafbaren Handlung ausgeht.

Zum Autor:**Dr. Martin Bahr**

ist Rechtsanwalt in der Hamburger Kanzlei Heyms & Dr. Bahr. Seine Interessenschwerpunkte sind Recht der Neuen Medien, Gewerblicher Rechtsschutz und Glücksspiel-/Gewinnspielrecht. Neben der reinen juristischen Befähigung besitzt der Anwalt vor allem auf dem Gebiet der Soft- und Hardware ausgezeichnete Kenntnisse und ist zudem langjähriger Dozent und Referent.

**RECHT****USA:****Vier Millionen Schadensersatz wegen Spam**

Ein Spammer wurde von einem kalifornischen Gericht dazu verurteilt, vier Millionen Dollar Schadensersatz an Microsoft zu zahlen.

Der Beklagte Daniel Khoshnood hatte eingetragene Marken von Microsoft als URLs von Landingpages verwendet. Angeschrieben hatte er unter anderem auch Hotmail-Adressen.

DATENSCHUTZ:**Persönliches Nutzungsverhalten darf nicht gespeichert werden**

Hilmar Schmudt hat in Spiegel-online einen ausführlichen Beitrag über des Thema „Spionagedienst eMail“ geschrieben. Wichtiger Tipp für Sie: Wenn Sie im Rahmen Ihres Newsletters Klickverhalten registrieren (und das sollten Sie), achten Sie unbedingt darauf, dass Ihre Software datenschutzrechtlich einwandfrei arbeitet. Konkret heißt das, dass Nutzerdaten (eMail-Adresse) und Nutzungsdaten (Klickverhalten) getrennt gespeichert werden müssen und nicht zusammengeführt werden dürfen.

Das Teledienstschutzgesetz schreibt dazu in § 6 Abs. 3: „Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 4 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.“

<http://www.spiegel.de/spiegel/0,1518,309439,00.html>

RETURNPATH:**Am besten Montag**

Der eMail-Dienstleister Returnpath hat 3,4 Millionen eMails aus 16.000 Kampagnen untersucht. Ergebnis: nicht Dienstag, sondern Montag ist der beste Versandtag. Samstag sollten Sie nichts senden.