Alternative zu Google Analytics

Flucht aus der Grauzone

Viele Nutzer von Google Analytics machen sich Sorgen: Wegen bestehender Rechtsunsicherheit steht die beliebte Web-Tracking-Lösung seit Längerem unter dem Beschuss deutscher Datenschützer. Während kleine Online-Shops bisweilen noch dazu neigen, den Ausgang dieses Rechtsstreits einfach abzuwarten, wird die unausgegorene Rechtslage für große Wirtschaftsunternehmen mittlerweile zum Problem.

Was für Online-Shops und professionelle Web-Seitenbetreiber längst ein unverzichtbares Instrument der täglichen Arbeit ist, nutzen inzwischen auch immer mehr große Wirtschaftsunternehmen: die Web-Analyse-Software Google Analytics. Gilt es doch, mit dem kostenlosen Tool des Marktfiihrers das Kaufverhalten ihrer Kunden nachhaltig zu erforschen und mithilfe der gesammelten Daten die eigene Angebotspalette und Gebrauchstauglichkeit optimal auf deren Wünsche abzustimmen. Doch seit gut zwei Jahren steht die beliebte Software nun im Brennpunkt teils emotional geführter Diskussionen um die Diskrepanz zwischen herrschender Gesetzgebung und tatsächlichem Nutzen.

Bereits im Januar 2009 bemängelte das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) die grundsätzliche Vereinbarkeit von Google Analytics und dem deutschen Datenschutzrecht. Und dies nicht nur aufgrund der beim Tracking gespeicherten IP-Adressen. Vor allem die Übermittlung der Analysedaten an Server außerhalb der EU, die unzureichende Möglichkeit zur Löschung der erhobenen Daten und die grundsätzliche Möglichkeit der Verkettung von Nutzerdaten zu einem umfassenden personalisierten Profil stimmten die Datenschützer bedenklich. Aufwind bekam die Diskussion nochmals durch ein im November 2009 veröffentlichtes Statement des Düsseldorfer Kreises zur datenschutzkonformen Ausgestaltung von Web-Analyse-Verfahren. Auf Grundlage des Telemediengesetzes (TMG) forderten Deutschlands oberste Datenschützer unter anderem die Einwilligung des Nutzers, um am Web-Analyse-Verfahren teilzunehmen. Im Mai 2010 nahm Google dann zwei Anpassungen in Google Analytics vor und reagierte damit auf die Forderungen der Datenwächter: Betreiber konnten durch eine Anpassung im Tracking-Code ihrer Web-Seite die gesammelten IP-Adressen durch eine teilweise Maskierung anonymisieren. Und ein von Google zur Verfügung gestelltes Plug-in gestattete dem Web-Seiten-Besucher, über ein Opt-out-Verfahren die Erstellung von Nutzerprofilen insgesamt zu unterbinden. Gleichwohl blieb ein großer Teil der Forderungen des Düsseldorfer Kreises offen. Zum einen war das Plug-in für eine Vielzahl von Browsern, wie etwa Opera und Safari, gar nicht verfügbar. Zum anderen blieb die Übertragung von Nutzerdaten an Server außerhalb der EU als elementarer Kritikpunkt nach wie vor bestehen. Folglich herrscht bis dato keine eindeutige Rechtsgrundlage, sodass momentan alle Beteiligten auf eine endgültige Entscheidung des Europäischen Gerichtshofs (EuGH) warten.

Zudem rät auch das Gros der auf Internet-Recht spezialisierten Anwälte derzeit von einer Verwendung von Google Analytics ab. Vor dem Hintergrund des Telemediengesetzes und den Äußerungen der Datenschützer könnten Bußgelder und Abmahnungen drohen, so die Warnung der Experten, auch wenn die Rechtslage nicht hundertprozentig eindeutig erscheint.

Kein Wunder also, dass mittlerweile viele Unternehmen über den Ausgang der kontrovers geführten Diskussionen verunsichert sind. Ob gezielte Marketingkampagnen mit Google Adwords, das Sammeln von Erkenntnissen zum Kaufverhalten von Kunden oder das Einstellen von Whitepapers mit Login, um an neue Interessentendaten zu kommen: Immer mehr Betriebe, die ihr unternehmensrelevantes Web-Tracking nicht länger auf rechtsproblematischem Niemandsland durchführen wollen, wechseln auf datenschutzkonforme Lösungen wie die hier weiter dargestellte Software Urchin - und kontrollieren mit den Pendants zu Google Analytics die umstrittenen Datenbestände künftig in eigener Regie.

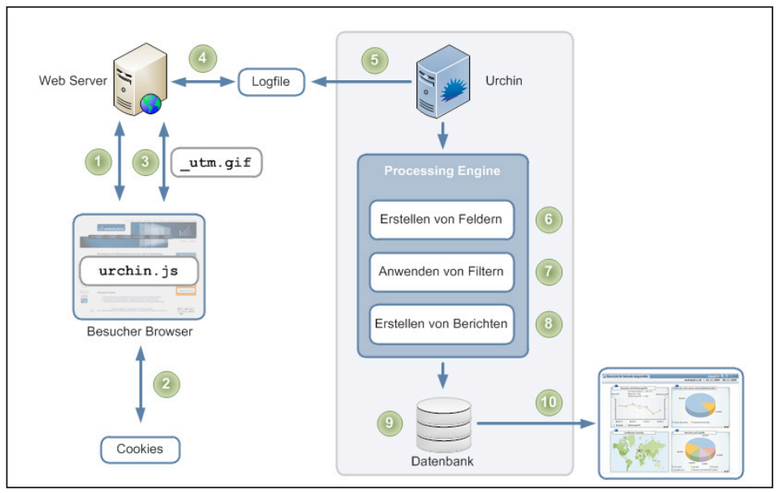

Bild 1. In ausgeklügelten Einzelschritten erfasst und verarbeitet das Urchin-System das Kundenver halten und bereitet es für die Darstellung auf.

Die kostenpflichtige Urchin-Software ist eine im Umfang mit Google Analytics vergleichbare Web-Analyse-Lösung, die jedoch beim Kunden installiert, gehostet und verwaltet wird. Somit befinden sich alle gesammelten und gespeicherten Daten abgeschottet auf unternehmenseigenen oder vom Unternehmen verwalteten Servern und bieten so im besten Fall keinerlei Angriffsfläche mehr für datenschutzrechtliche Bedenken. Da sämtliche Daten ausschließlich auf eigenem Equipment vorgehalten, verarbeitet und ausgewertet werden, bleiben die Bestände grundsätzlich in Deutschland beziehungsweise in Europa, und der Website-Betreiber kann über das ausgefeilte Konten-, Nutzer- und Gruppen-Management sicherstellen, dass kein Unbefugter Zugriff auf die Daten nehmen kann.

Für Website-Betreiber ist damit jeglicher Ärger vom Tisch. Von den fünf Kritikpunkten des Düsseldorfer Kreises liegen nämlich nur zwei ganz spezielle Forderungen in der direkten Verantwortung des Betreibers und dessen technischen Gegebenheiten - unabhängig davon, welche Analysesoftware er auch immer einsetzt: das Widerspruchsrecht und der gewünschte Hinweis zur Erstellung pseudonymer Nutzungsprofile. Um diesen Erfordernissen zu genügen, kann der Betreiber einer Website dem Besucher ganz gezielt eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einräumen - ein so genanntes Opt-out, indem er eine Schaltfläche oder Checkbox auf der Website integriert. Diese würde dann nach Betätigung die Ausführung eines Tracking-Codes verlässlich unterbinden. Eine elegante Lösung dazu bietet etwa das Browser-Add-on „Opt-Me-Out“, das kostenlos unter http://www.opt-me-out.de heruntergeladen werden kann. Und was den datenschutzrechtlichen Hinweis bezüglich der Erstellung pseudonymer Nutzungprofile angeht, obliegt es ebenfalls dem Betreiber, einen entsprechenden Passus in die Datenschutzerklärung zu integrieren. Dabei sollte er sich an einen kundigen Rechtsanwalt wenden, der ihm wiederum eine geeignete Formulierung an die Hand gibt.

Alles andere ist bei Urchin obligatorisch – auch die von Datenschützern so vehement geforderte Datentrennung oder die Anonymisierung oder Löschung von IP-Adressen. Zwar ist das von Datenschützern vorgebrachte Argument des Personenbezugs von IP-Adressen in Zeiten von dynamischen IPs und dem Einsatz von Routern mit NAT (Network Address Translation) aus technischer Sicht nur schwer nachvollziehbar. Zum einen, weil die eigentliche IP-Adresse des individuellen Besuchers einer Web-Seite hinter einem Router gar nicht sichtbar ist. Zum anderen ist in Deutschland eine Feststellung der Person anhand einer IP-Adresse nur durch einen Richterbeschluss bei schwerwiegenden Straftaten möglich. Bei Urchin jedenfalls können IP-Adressen sowohl anonymisiert als auch durch passende Filtersetzung jederzeit von der Datenverarbeitung aus geschlossen werden. Zudem lassen sich Datenbestände mit wenigen Mausklicks löschen. Eine Datentrennung ist primär schon dadurch gegeben, dass ein Nutzer sich auf einer Website nicht zwangsläufig zu erkennen geben muss. Dies ist immer nur dann der Fall, wenn sich beispielsweise der Nutzer zum Betreten eines geschlossenenBereichs oder beim Checkout-Prozess eines Online-Shop-Kaufs anmelden müsste. Aber selbst wenn dies der Fall ist, werden die Anmeldedaten nicht im Webserver-Logfile vermerkt, da eine Verknüpfung von User-Daten und Profil bei Urchin per Design nicht möglich ist.

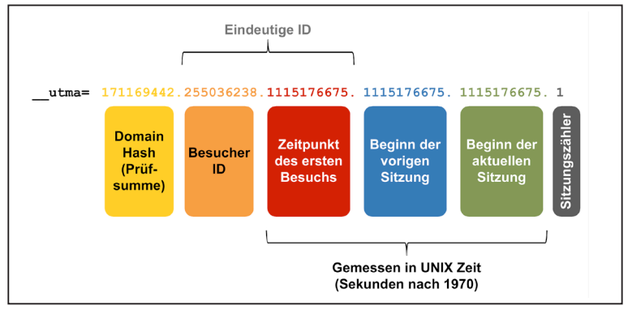

Bild 2. Die Identifikation im _utma Cookie in Urchin unterscheidet lediglich zwischen neuen und wiederkeh renden Besuchern.

Fazit

Als datenschutzkonformes Pendant zu Google Analytics bieten Lösungen wie Urchin die in Wirtschaftsunternehmen benötigte Rechtssicherheit bei der professionellen Web-Analyse. Wie Google Analytics helfen sie allen Website-Inhabern, ihre Online-Marketing-Initiativen, Website-Zugriffsmerkmale und das Suchverhalten ihrer Kunden besser zu verstehen. Doch anders als Google Analytics liefert etwa Urchin tiefer gehende Ergebnisse, einschließlich Bilder, Downloads, Roboter, Statuscodes (etwa 404, 500) und Verweisfehler, darunter auch veraltete Links. Mehr noch: Da die Lösung Server-Protokolldateien als primäre Datenquelle verwendet, kann das Tool auch in Anwendungen zum Einsatz kommen, die sich nicht für einen gehosteten Service wie Google Analytics eignen, wie etwa das Tracking der Zugriffe auf ein Firmen-Intranet, die erneute Verarbeitung älterer Protokolldateien oder Berichte zu Server-Fehlern. Vor allem aber - unabhängig von der Datenschutzkonformität - behalten Unternehmen die unumschränkte Macht über ihre gesammelten Informationen, da alle Daten ausschließlich auf eigenem Equipment erhoben, vorgehalten, verarbeitet und ausgewertet werden. Holger Tempel/jos

Holger Tempel ist Geschäftsführer von Webaltics.