

Gute Bots und böse Bots: Wie sie den E-Commerce verändern

Wenn man in ‚gute‘ Bots und ‚böse‘ Bots unterteilen möchte, so kann man sagen, dass gute Bots Dienste für ihre Betreiber unternehmen und so zum Beispiel Zeit bei der Recherche sparen. Sie ziehen sich öffentlich zugängliche Informationen aus Websites heraus und sammeln diese. Um die Werbeindustrie nicht zu schädigen und um in den Website-Analyseprogrammen die Statistiken nicht zu verfälschen, geben sich die gutartigen Bots zu erkennen. Böse Bots sind Programme, die zum Beispiel Schadsoftware ohne Wissen und Zustimmung des Nutzers installieren oder den Traffic einer Website so manipulieren, dass dadurch der Werbeindustrie Schaden zugeführt wird. Einige Beispiele:

Spider Bots (Crawler)

Crawler sind Bots, die das Web nach HTML-Dokumenten durchforsten und dafür sorgen, dass zu Suchanfragen die passenden Ergebnisse ausgeliefert werden.

„Gute“ Variante: Crawler gibt sich in Logfiles als solcher zu erkennen und hält sich beim Indizieren an die Vorgaben der Webseite, die in robots.txt hinterlegt sind. Ad Serving und Ad Verification Systeme können ohne viel Aufwand die Seitenaufrufe als Invalid Traffic (hinsichtlich der Werbeauslieferung) herausfiltern.

„Böse“ Variante: Crawler halten sich nicht an die oben benannten Vorgaben. Werbeauslieferungen können fälschlich als „Valid Traffic“, also gültige Website-Aufrufe, verbucht werden.

Trader Bots

Trader Bots sind Suchmaschinen, die gezielt nach den günstigsten Preisen suchen. Sie durchforsten zum Beispiel Online-Marktplätze oder einzelne Händler. Dadurch können E-Commerce-Unternehmen ihre Wettbewerber beobachten und Preise optimieren.

„Gute“ Variante: Trader Bots halten sich an die Vorgaben für Bots (siehe oben unter „Spider Bots“) und verstoßen nicht gegen Nutzungsbestimmungen der Webseitenbetreiber.

„Böse“ Variante: Trader Bots halten sich nicht an die Vorgaben für Bots (siehe oben unter „Spider Bots“) und/oder verstoßen gegen Nutzungsbestimmungen und Schutzrechte der Webseitenbetreiber.



Chatbots

Mit den immer intelligenter werdenden Chatbots lässt sich ein Teil der Kundenkommunikation von Unternehmen auslagern und automatisieren. Vor allem häufigere und einfachere Anfragen können so kostensparend beantwortet werden.

„Gute“ Variante: Chatbots halten sich an die Vorgaben für Bots (siehe oben unter „Spider Bots“), verstoßen nicht gegen Nutzungsbestimmungen der Webseitenbetreiber, informieren Nutzer sachdienlich und geben sich als Chatbots für den Nutzer zu erkennen.

„Böse“ Variante: Chatbots halten sich nicht an die Vorgaben für Bots (siehe oben unter „Spider Bots“), verstoßen gegen Nutzungsbestimmungen der Webseitenbetreiber, verbreiten absichtlich Fehlinformationen und/oder geben sich nicht für den Nutzer zu erkennen.

Scraper Bots

Diese Bots werden für das Einsammeln aber auch für den Diebstahl von Inhalten eingesetzt. Bilder und Texte werden abgezogen, um an anderer Stelle dupliziert beziehungsweise missbraucht zu werden.

„Gute“ Variante: Scraper Bots halten sich an die Vorgaben für Bots (siehe oben unter „Spider Bots“) und verstoßen nicht gegen Nutzungsbestimmungen und Schutzrechte der Webseitenbetreiber.

„Böse“ Variante: Scraper Bots halten sich nicht an die Vorgaben für Bots (siehe oben unter „Spider Bots“) und/oder verstoßen gegen Nutzungsbestimmungen und Schutzrechte der Webseitenbetreiber.

Spam Bots

Spam per E-Mail hat in den vergangenen Jahren immer mehr zugenommen. Leider werden die Spam Bots auch immer klüger, sodass die E-Mails es auch immer wieder mal am Spam-Filter vorbei ins Postfach schaffen, ohne dafür die Zustimmung des Nutzers zu haben.

Im Bereich Werbung beispielsweise werden bösartige Bots eingesetzt, um Werbekontakte oder Clicks zu simulieren, die gar nicht real sind. Werbeflächen können von nahezu jedem Webseitenbetreiber zur Verfügung gestellt werden. Hierfür werden die Seiten Werbeflächenvermarktern angeboten oder bei automatisierten Vermarktungsplattformen angemeldet.



Aber nicht jede Website erzeugt ausreichend Traffic, damit durch die Werbeflächen Geld verdient werden kann. Will ein Webseitenbetreiber künstlich den Traffic auf der Seite und die Klicks auf die Werbemittel erhöhen, so programmiert oder beauftragt er einen Bot, der diese Seiten künstlich ‚besucht‘ und dabei auch ab und an einen Klick auf ein Werbemittel auslöst. Damit der Bot-Anteil der Werbekontakte und Klicks von den Analysetools der Werbekunden nicht anhand der offiziellen IAB-Bot-Liste¹ rausgefiltert werden kann, gibt sich der Bot nicht zu erkennen und ahmt zum Beispiel menschliches Verhalten nach. „Am Ende wird dem buchenden Werbekunden eine Rechnung über die Werbekontakte gestellt, die jedoch zum Großteil nicht von Menschen erzeugt wurden. Er bezahlt also zu viel Geld.

Um solche bösartigen Bots zu erkennen, wurden in den letzten Jahren zahlreiche Systeme programmiert, die zum Beispiel nach typischen Mustern suchen. Da die bösartigen Bots immer raffinierter werden und das Verhalten von Menschen zum Teil sehr gut nachahmen können, findet ein regelrechter Wettlauf zwischen den Entwicklern dieser Bots und den Entwicklern der Tools statt, die gegen Bots schützen sollen.

Auch für die Markt- und Meinungsforschung im politischen Bereich kann die Entwicklung von bösartigen Bots fatale Folgen haben. Wenn man sich nicht mehr sicher sein kann, ob der Website-Traffic von Menschen oder von Bots stammt, wird es schwieriger, ein realistisches Meinungsbild zu erhalten.

Oktober, 2018

Autoren:

Andreas Hamdorf (pilot Hamburg), Stellvertretender Vorsitzender der Fokusgruppe Digital Marketing Quality im BVDW

Philipp von Hilgers (Meetrics), Stellvertretender Vorsitzender der Fokusgruppe Digital Marketing Quality im BVDW

¹ <https://www.iab.com/guidelines/iab-abc-international-spiders-bots-list/>

