Gekaufte Likes

„Social Bots“ sind Computerprogramme, die in den sozialen Medien automatisch antworten und liken. Problematisch ist das, wenn sie zur Meinungsbeeinflussung eingesetzt werden.

Eintausend neue Follower für 10 Euro. Wer regelmäßig auf *Instagram, Facebook* und *Youtube* unterwegs ist, kennt diese Anzeigen. Klicks und Likes sind die Währung des Internets. An ihnen werden der Erfolg und die Popularität von Einzelnen und Organisationen gemessen. Aus dieser Abhängigkeit hat sich ein eigener Geschäftszweig entwickelt. In Asien, vorwiegend in Indien und Bangladesch, gibt es „Klickfarmen“, wo Menschen täglich vor Computerbildschirmen sitzen, eine Vielzahl an Social-Media-Profilen anlegen und damit liken, folgen und kommentieren. Es gibt auch Computerprogramme, die automatisiert „Fans“ erzeugen. Darauf sind diverse Social-Media-Plattformen allerdings schon so weit sensibilisiert, dass *Facebook* und *Instagram* in den vergangenen Jahren in groß angelegten Aktionen mehrere Tausend der gefälschten Konten löschen konnten.

Manipulation. Problematisch wird die Sache mit den gekauften Freunden, wenn sie zur Beeinflussung von Meinungen oder menschlichem Verhalten eingesetzt werden. „Das funktioniert sehr gut, weil wir Menschen soziale Wesen sind. Wir lassen uns von der Tatsache, dass mehrere Mitglieder unseres Netzwerks etwas Bestimmtes kaufen oder tun, sehr leicht beeinflussen“, erklärt IT-Blogger Philipp Schaumann *(sicherheitskultur.at)*. „Wir haben es mit automatisiertem Social Engineering zu tun, nämlich dem aktiven Verändern des Verhaltens einer großen Zahl von Menschen.“ Dieses Vorgehen könne von politischen Parteien instrumentalisiert werden, die ihre Inhalte mithilfe von Social Bots verbreiten. Dieses Problem würde sich durch die „Filterblasen“ noch weiter verstärken.

Roboter-Programme sind auf Signalwörter programmiert und reagieren autonom auf Social-Media-Meldungen.

Wahlen. Die Universität von Oxford hat eine Studie über den amerikanischen Präsidentschaftswahlkampf 2016 veröffentlicht mit dem Ergebnis, dass sich beide Kandidaten, Hillary Clinton und Donald Trump, der Social Bots bedient haben sollen. „Bei der ersten TV-Debatte am 26. September 2016 ist jeder dritte Tweet – 37,3 Prozent – zur Unterstützung von Trump von einem Software-Roboter abgesetzt worden“, sagt Schaumann. „Bei Hillary Clinton lag der Bot-Anteil bei 22,3 Prozent. Ein Drittel der Follower beider Kandidaten sind keine echten Menschen, sondern Roboter.“ Die Gefahr liegt darin, dass es sich bei vermeintlichen Meinungsführern um Computerprogramme handelt, die Trends vorgeben und durch ihre große Anzahl andere Äußerungen aus der öffentlichen Meinung verdrängen.

Falschmeldungen. Auf *Twitter* werden Bots so programmiert, dass sie bestimmte Meldungen zu einem Hashtag (Meta-Links) veröffentlichen. Bei diesen Meldungen handelt es sich in einigen Fällen um Information aus ungesicherten Quellen, die so lange und so oft geteilt werden, bis User von deren Wahrheitsgehalt überzeugt sind und sie weiterverbreiten.

Auch das Social-Media-Team des Innenministeriums hat bereits Erfahrungen mit dieser Art von Falschmeldungen gemacht. Ende Juli 2017 wurde auf *Facebook* und *Twitter* eine Meldung verbreitet, in der angebliche Personentransporte über die Brennergrenze beschrieben wurden, bei denen mehrere Hundert Schwarzafrikaner illegal nach Österreich eingeschleust worden sein sollten. Dazu gab es ein Video, das Menschengruppen neben einer befahrenen Straße zeigte. Obwohl es sich offensichtlich nicht um ein österreichisches Straßenbild handelte und die Meldung über die Personentransporte jeglicher Grundlage entbehrte, wurden die Inhalte weiterverbreitet. Das Social-Media-Team des Innenministeriums veröffentlichte auf *Facebook* und *Twitter* eine Richtigstellung, die von Usern geteilt wurde und auch von den klassischen Medien übernommen wurde.

Unternehmen. Auch *Facebook, Twitter* und Co. haben ein Interesse daran, gegen die Social Bots vorzugehen, da sie gegen die Nutzungsbedingungen verstoßen und die Authentizität der Netzwerke untergraben. User können die Fake-Profile melden, außerdem sollen die Netzwerke Anomalien und Muster erkennen.

Anna Strohdorfer

SOCIAL BOTS

Manipulationen

- *Profilbilder:* Einen Fake-Account erkennt man daran, dass es maximal ein bis zwei Fotos gibt, auf denen Menschen zu sehen sind.
- *Timeline:* Ein Account, der erst seit Kurzem besteht, aber viele und thematisch gleiche Inhalte zu jeder Tages- und Nachtzeit postet, könnte ein Social Bot sein.
- *Sprache:* Da es sich meistens um einfache Computerprogramme handelt, kann ein geringer Wortschatz und die Unfähigkeit, auf komplexe Fragen zu reagieren, auf einen Social Bot hindeuten.

FOTO: TIAGOZR/FOTOLIA