Hallo! Sind Sie ein Bot oder ein Mensch?
Fünf Tipps für die Kommunikation in sozialen Netzwerken

Die Kommunikation in sozialen Netzwerken hat so ihre Tücken. Bots sind eine davon. Das muss sich gerade auch Twitter eingestehen. Doch wie erkennt man, ob das Social-Media-Gegenüber ein Mensch oder eine Maschine ist? Sophos Sicherheitsexperte Michael Veit hat fünf Kriterien für einen Bot-Check zusammengefasst.

Die Social-Media-Plattform Twitter hat ein Bot-Problem. Der Microblogging-Dienst steht seit einiger Zeit unter wachsender Beobachtung. Der Verdacht: Hunderttausende von Accounts, die legal realen Personen zu gehören scheinen, könnten in Wirklichkeit „Bots" sein. Ein Bot ist ein Computerprogramm, das weitgehend automatisch wiederholende Aufträge umsetzt, ganz ohne menschliche Eingriffe. Diese massenweise aufgesetzten und automatisierten Accounts sollen die Plattform fluten. Wozu? Meist, um politische Ansichten zu unterstützen.
Zahlreiche Beschuldigungen stehen im Raum, dass das englischsprachige Twitter-Universum mit Bots aus Staaten wir Russland überflutet wird. Ziel sei es, etwa den Brexit in UK zu unterstützen, Präsidentenkandidaten in den USA zu pushen oder zu verunglimpfen. Kürzlich bemerkten viele bekannte – und dem rechten politischen Lager zugehörige – Profile, dass ihre Twitter-Accounts eingefroren wurden und ihre Follower-Zahl stark abfiel, zusammengefasst unter dem Hashtack #TwitterLockOut. Waren das echte Accounts? Oder hat Twitter hier Bot-gesteuerte Accounts aufgeräumt? Ein konkretes Statement dazu gab es nicht.

Bis zu 15 Prozent aller Twitter-Accounts sind Bots
Bots sind einfach zu erstellen und sehr effektiv darin, alles mit Propaganda zuzupflastern, um Diskussionen zu beeinflussen und die Bevölkerung zu splitten. Sie sind in ihrer Wirkung nicht zu unterschätzen. Laut einer Studie von 2017 sollen Bots bis zu 15 Prozent aller Twitter-User (rund 30 Millionen) ausmachen. Doppelt so viele, wie Twitter selbst einschätzt.

Bots sind keineswegs nur darauf reduziert, beispielsweise Amerikas Rechtsstehende auf Twitter zu unterstützen. Sie sind ein Thema auf allen großen Social Media Plattformen, auch Facebook und Instagram, in nahezu allen Ländern und Sprachen. Wenn man als User in sozialen Netzen unterwegs ist, sollte man sich selbst fragen: „Würde ich erkennen, ob ich mit einem Bot kommuniziere?" „Die Entwickler werden jeden Tag kreativer. Es ist nicht immer auf den ersten Blick erkennbar, ob man mit einem Bot oder einer echten Person kommuniziert", klärt Michael Veit, Technology Evangelist Sophos, auf.

Beim nächsten Social-Media-Geplauder sollten Nutzer ihr Gegenüber auf folgende fünf Anzeichen überprüfen:

- Wenn der Account für sich beansprucht, einen bedeutenden Politiker oder einen Prominenten zu repräsentieren, gilt es zu verifizieren, ob es sich hierbei nicht um einen Nachahmer handelt. Es gibt ein blaues „Verifizierungs"-Häkchen, das Twitter denjenigen Accounts verleiht, die sich als echt bewährt haben. Allerdings existiert dieser Check nicht für alle offiziellen Accounts. Dennoch, danach Ausschau halten, kostet nichts.
- Ein Account, der nur das generell blanke Profilbild von Twitter verwendet (früher war es das „Ei") und einen kryptischen User-Namen (Manfred25486589) nutzt, ist sehr wahrscheinlich ein Bot.
- Auch ein auf den ersten Blick plausibles Profilfoto kann irreführend sein. „Viele Bots schnappen sich Fotos von anderen Social Media Accounts oder haben einen eigenen Vorrat an Bildern, um ihren Profilen ein authentisches Äußeres zu geben", so Veit. „Kurz das Profilbild, dem man misstraut, auf Google suchen – vielleicht wird es ja mit

einem völlig anderen Namen in Zusammenhang gebracht, dann weiß man bereits, woran man ist“.

- Einer der neuesten Tricks von Twitter Bots sind auf den ersten Blick glaubwürdig erscheinende Biografien (also der beschreibende Text unter dem Profilname). Hier sollte man darauf achten, ob das Bild zu dieser Beschreibung passt. Ein Beispiel: Junge Frau im Bikini als Profilfoto mit Account-Beschreibung „Großmutter von Fünfen, hingebungsvoller Ehemann“. Passt nicht zusammen – ein Hinweis für einen Bot.
- Man sollte auch etwas genauer auf das Verhalten des Users schauen: beschäftigt sich der Nutzer in den Gesprächen mit anderen auf eine sinnvolle Weise oder spuckt er nur Aussagen, Hashtags und Links ohne reale Interaktion aus? Es gibt zwar mittlerweile auch hochentwickelte Bots, deren Konversation einer wirklichen Frage-Antwort-Konversation ähnelt, aber die meisten Bots, die Twitter überschwemmen, sind eher Spam-artig. Wer auf einen Bot-Tweet antwortet, wird ziemlich sicher keine sinnvolle Reaktion erhalten.

Der Markt bietet Werkzeuge und Webseiten, die Bot-Aktivitäten auf Twitter verfolgen und sogar Accounts untersuchen, ob sie Bots sind. „Diese Maßnahmen können praktisch sein, den eigenen Verdacht zu verifizieren. Allerdings sollte man sich immer darüber bewusst sein, dass ein derartiges Tool eben auch das Werk seines Entwicklers ist, sprich: ein Bot-Checker kann einerseits seriös und vertrauenswürdig sein, oder aber auch seine eigene politische Agenda haben“, so Veit. „Am Ende gilt: auf Bauchgefühl und gesunden Menschenverstand achten. Man merkt schnell, wenn eine Konversation seltsam verläuft. Spätestens dann sollte der User sehr vorsichtig sein und gegebenenfalls den verdächtigen Account der Social-Media-Plattform melden. Nur so bleibt die Interaktion im Netz echt.“

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de