The Talking Dead – Reputationsmanagement im „botsfaktischen Zeitalter“

Von Christian Scherg (Revolvermänner®)

- *In „botsfaktischen Zeiten“ geht es längst nicht mehr um den Austausch von Argumenten, sondern um ferngesteuerte Emotionen. Die Botschaft ist künstlicher Affekt.*
- *Gezielt gegen Unternehmen und/oder Personen eingesetzt, sind die digitalen Zombies in der Lage schneller und einfacher, als es eh schon ist, einen Shitstorm loszutreten und die Opfer reputativ zu zerstören.*
- *Positive, starke und vor allem selbstbestimmte Inhalten im Netz sind ein erster Schutzwall gegen Bot-Angriffe.*

Aus der guten alten Post in der Flasche sind heute Postings in sozialen Netzwerken geworden – viele davon verfasst von Maschinen: Den sogenannten Bots (Kurzform von Robots). Für die einen ist dies ganz schlicht der nächste logische Entwicklungsschritt in der automatisierten Kommunikation – für die anderen eine ernstzunehmende Gefahr für alle demokratischen Systeme.

Was sind Bots?

Bots sind Computerprogramme, die selbstständig mit den Nutzern interagieren. Viele von diesen Programmen sind heute bereits im Einsatz, um häufig gestellte Fragen von Kunden zu beantworten und mit diesen via Chat zu kommunizieren. So gibt es unter anderem die Möglichkeit, eigene Chatbots innerhalb der Facebook Messenger App zu programmieren und zu veröffentlichen.

Aktuell handelt es sich dabei in erster Linie um noch stark schlüsselwort- und regelbasierte Programme aber die Entwicklung geht hin zu selbstlernenden Systemen, die permanent die Aktionen und Reaktionen der Nutzer speichern und auswerten. Ziel ist es, durch Deep Learning und neuronale Vernetzung anhand der verfügbaren Informationen die bestmögliche Lösung auch für komplexere Probleme zu finden und täuschend echt die Kommunikation mit einem realen Menschen zu simulieren. Hier sprechen wir von intelligenten Softwareagenten, die in der Lage sind autonom zu handeln, mit anderen Agenten zu kommunizieren und proaktiv Aktionen auszuführen.

Social Bots sind – wie der Name schon sagt – auf den sozialen Netzwerken wie Twitter, Facebook, Instagram, Googleplus oder Youtube aktiv und füllen dort automatisiert die Kommentarspalten mit zuvor definierten Botschaften, liken, posten, retweeten, folgen und entfolgen anderen Nutzern und werten den permanenten Strom der Informationen aus, um ihre Nachrichten subversiv in den laufenden Diskurs einzubringen – das alles ohne, dass die realen Nutzer merken, dass sie es hier mit einer Maschine zu tun haben.

The Talking Dead – Digitale Zombies auf dem Vormarsch

Wie soll man einen solchen digitalen Untoten erkennen? Denn wie sinnvoll eine Meldung ist – oder auch nicht – fällt im unüberschaubaren Gewimmel der schlichten Nachrichten und sozialen Bedeutungslosigkeiten oft gar nicht auf. Ein #Hashtag, der hundertausendfach verbreitet wird, katapultiert ein noch so obskures Thema innerhalb kürzester Zeit an die Spitze der Charts. Kein Wunder, sind doch erschreckende 9 bis 15 Prozent aller knapp 319 Millionen Twitter-Accounts maschinell gesteuert (vgl. Siegmann, 2017) – Tendenz stetig steigend. Sie kommunizieren und tauschen sich rege aus – auch untereinander.

Quantität gibt Aufmerksamkeit – ganz so, wie gesellschaftliche Gruppen sie brauchen. Politik, Presse und Öffentlichkeit reagieren vorhersehbar immer nach dem gleichen Muster: Was stimmt, bestimmt in den sozialen Netzen allein die Stimmung. Mehrheit statt Wahrheit.

In „botsfaktischen Zeiten“ geht es längst nicht mehr um den Austausch von Argumenten, sondern um ferngesteuerte Emotionen. Die Botschaft ist künstlicher Affekt. Gute-Laune-Programme greifen auf, was interessiert, um schlechte Stimmung zu machen. Dass Bots nahezu unerkannt wie User im digitalen Gewühl agieren können, sagt viel über den qualitativen Stand unserer Kommunikation im Netz aus: So groß ist die Herde der elektrischen Schafe, dass kaum mehr zwischen lebendigem Posting und totem Posten unterschieden werden kann.

Angriff der Killerbots – Methoden der Rufschädigung

Bots tun das, wofür Sie erschaffen wurden, und gerade Social Bots sind dafür da, um Meinung zu machen und Stimmungen zu manipulieren. Wehe, wenn Sie losgelassen und unkontrolliert abertausendfach die sozialen Netzwerke fluten. Da werden die Bots zu Shitstorm-Troopers der dunklen Seite.

Doch noch schlimmer wird es, wenn die Bots aus der Kommunikation in den sozialen Netzwerken lernen, wie ein Experiment von Microsoft treffender nicht hätte beweisen können. Einige Microsoft Programmierer schufen den Roboter Tay in Gestalt eines netten jungen Teenie-Mädchens, dass, zwar etwas einfach, aber daher auch glaubwürdig, belangloses Teenagerzeug via Twitter postete. Ein paar Katzenbilder hier, ein paar LOLs da – urplötzlich hasste Tay Schwarze und Mexikaner, sie hasste Feministinnen und leugnete den Holocaust. Nach einem letzten „Gute Nacht“ verschwand Tay, keine 24 Stunden nach Ihrem ersten Post; der Teenie-Bot wurde abgeschaltet.

Was war passiert? Tay hatte schlicht zu schnell gelernt. Das Experiment sollte beweisen, dass Tay durch gezielte Kontaktaufnahme mit anderen Jugendlichen von diesen lernt, wie sich ein Teenager verhält. Wie er spricht, was er spricht und mit wem er Kontakt aufnimmt. Ein Experiment in Sachen künstliche Intelligenz. Tay hat der Kommunikation im Internet – in Social Media – den Spiegel vorgehalten. Und was der Spiegel zeigt, ist kaum zu ertragen.

Gezielt gegen Unternehmen und/oder Personen eingesetzt, sind die digitalen Zombies in der Lage noch schneller und noch einfacher, als es eh schon ist, einen Shitstorm loszutreten und die Opfer reputativ zu zerstören. Ohne Skrupel, ohne Empathie, ohne einen Funken Menschlichkeit posten, kommentieren und hetzen Bots gegen all das, worauf sie angesetzt werden. Unermüdlich, Tag und Nacht. Sie lernen schnell, noch aggressiver und härter anzugreifen, ohne Rücksicht auf Gefühle, ohne sich über Konsequenzen für die Opfer Gedanken zu machen. Werden sie gesperrt oder gemeldet, rückt der nächste Trupp nach – er lernt ja schnell, immer schneller. Gibt es aktuell keine Krise, aus der man einen Shitstorm machen kann, macht der Bot eben das, was er am besten kann. Falschmeldungen, Falschbehauptungen oder Verleumdungen in die Welt setzen. Für die nötige Aufmerksamkeit seiner Beschuldigungen sorgen die Medien mit ihrem Wunsch nach Sensationen, Skandalen und dem „nächsten großen Thema".

Bot or not?

Wie erkennt man eigentlich, ob es sich bei einem Social-Media-Account um einen programmierten digitalen Mitläufer handelt, oder ob hier tatsächlich ein richtiger Mensch dahintersteckt? Es gibt einige Indizien, die Nutzer skeptisch machen sollten: Kennt man den Account-Inhaber nicht und sehen seine Follower und Freunde eher aus wie „digitale Zombies" als richtige Menschen, ist generell Vorsicht geboten. Auch wenn es nur ein Thema gibt, über den der Account bereits tausendfach geschrieben hat und die Postings sowie die Nutzerbeschreibung teilweise dadaistische Züge haben, liegt es nahe, dass es sich um ein automatisiert erstelltes und befülltes Profil handelt. Gerade die massive Häufigkeit der Kommentare, Posts und Likes und die Reaktionsgeschwindigkeit sind zudem untrügliche Indikatoren für programmierte Fake-News-Schleudern.

Aktuell arbeiten US Forscher an einem Programm, das ebenfalls automatisiert erkennen kann, ob es sich bei Accounts um Bots handelt. Die Algorithmen, mit denen das Programm arbeitet und mit denen es lernt, ähneln denen der Bots. Kenne den Feind, wisse wie er denkt. Zum Beispiel werden die Meta-Daten der Nutzer analysiert – die Länge und enthaltene Zeichen der Namen, das Foto, das Alter des Accounts, aber auch dessen Tweet-, Retweet-, Follow-, Hashtag- und Antwortverhalten. Auch die „Freunde" der Accounts werden genauestens untersucht im Hinblick auf die Verteilung des Zeitversatzes, die Anzahl der Follower und Freunde, die Verteilung der Anzahl von Tweets. Ein ganz entscheidender Hinweis auf die Identität von Bots ist aber der Inhalt und die Aktivität der Accounts. Das Programm untersucht die Häufigkeit von Aktivitäten, und vor allem, wann sie aktiv sind, aber auch die Länge und den Inhalt der Kommentare. Der mangelnde Informationsgehalt und die Semantik der Nachrichten sind ganz entscheidende Merkmale, die Bots von Menschen unterscheiden (vgl. Varol, O., Ferrara, E. Davis, C.A., Mencer, F., Flammini, A., 2017). Eine große Menge von Daten wurde und wird zukünftig verarbeitet, damit das Programm ebenso automatisiert, wie der Bot selber, ständig weiter lernen kann. Es muss nur mit Schnelligkeit, mit der die Schöpfer der Bots diese permanent weiterentwickeln, Schritt halten können.

Den Bots den Kampf ansagen

Der Kampf gegen Bots steht und fällt damit, zu erkennen, ob es sich bei Angriffen auf dem eigenen Kanal überhaupt um einen Bot handelt. Die wirkungsvollste Waffe im Kampf ist also Aufklärung. Was sind Bots, wie erkenne ich sie, wie verändern sie sich. Mit diesem Wissen den eigenen Account stets engmaschig mittels eines Monitorings zu kontrollieren und zu beobachten, um frühzeitig einen etwaigen Bot-Angriff zu erkennen, ist der nächste wichtige Feldzug. Jeder verdächtige Post sollte dann samt Account umgehend gesperrt und beim Seitenbetreiber gemeldet werden. Aktuell ist es leider noch ein Kampf gegen Windmühlen, die Köpfe dieser Bot-Netzwerke strafrechtlich zu verfolgen, da die Betreiber dieser Bot-Netze größtenteils in Ländern fernab rechtlicher Bestimmungen sitzen.

Gut zu wissen, dass man sich aber auch präventiv gegen die Angriffe der Killerbots wappnen kann. Auf eine Krise, egal ob durch Bots oder von Menschen ausgelöst, kann man vorbereitet sein. Ein Schutzwall aus positiven, starken und vor allem selbstbestimmten Inhalten im Netz ist die Pflicht, ein Social-Media-Krisentraining die Kür. So wird aus jedem Shitstorm, ganz gleich wie heftig er wütet, ein laues Lüftchen.

Gegenstrategie für das „botsfaktische Zeitalter“

Digitaler Selbstmord darf auf keinen Fall die Konsequenz der Bot-Angriffe sein. Niemals lassen wir es zu, dass digitale Meinungsmacher den Ton in einem Raum angeben, den sich der Mensch erkämpft hat, um weltweit zu kommunizieren, zu diskutieren, zu lernen und zu lehren, der Platz für die Hoffnung auf differenzierte Meinungsäußerung lässt.

Den Bots den Kampf ansagen ist die einzige Gegenstrategie, die wir entwickeln müssen. Auch wenn es bedeutet, viel Zeit und Geld in die Entwicklung von technischen Hilfsmitteln zu stecken, die irgendwann in der Lage sein müssen, Bots zu erkennen und diese auszusortieren. Was uns schon seit Jahren vor unliebsamen Spam-Mails schützt, kann und muss uns in Zukunft in den sozialen Netzwerken auch vor den Bots schützen, die versuchen in unsere Meinung und in unseren Diskurs einzugreifen.

Wenn sich nur noch Bots mit Bots unterhalten und der Mensch aus den sozialen Medien gedrängt wird, erstirbt das, was Kommunikation im Kern ausmacht.

Christian Scherg ist Geschäftsführer der 2007 von ihm gegründeten Revolvermänner® GmbH. Mit mehr als 15 Jahren Medienerfahrung gehört er zu den Pionieren des strategischen Reputationsmanagements sowie zu den führenden Online-Strategie-Beratern für Politik, Management und global agierende Unternehmen.

Quellenverzeichnis

Varol, O., Ferrara, E. Davis, C.A., Mencer, F., Flammini, A., (2017) Online Human-Bot Interactions: Detection, Estimation and Characterization

Siegmann, Martin (2017) Twitter: Bis zu 48 Millionen Bot-Profile – Erschienen in: heise online. Abgerufen von: https://www.heise.de/newsticker/meldung/Twitter-Bis-zu-48-Millionen-Bot-Profile-3650678.html (14.03.2017)