TAGESSPIEGEL
BACKGROUND

Cybersecurity

Was Unternehmen gegen Desinformation tun können

Wettbewerb zwischen Unternehmen kann viele Formen annehmen, darunter auch unfaire und illegale wie mit Hilfe von Desinformation. Denn Desinformation wird nicht nur im politischen Kontext genutzt, sondern auch im Konkurrenzkampf um Kund:innen.

von **Ulrich Hottelet**

veröffentlicht am 24.08.2023

Das gezielte Verbreiten falscher Informationen gibt es schon lange, aber die sozialen Medien haben die Möglichkeiten dynamisiert. Man unterscheidet je nach ihren Zielen **drei Arten der Desinformation**: erstens die generelle Rufschädigung, zweitens die gegen Produkte gerichtete, die angebliche Fehler oder schlechte Qualität anprangert, und drittens die gegen Personen im Unternehmen, in der Regel führende Manager:innen. Oft geht eine **feindliche Übernahme der Accounts** in sozialen Medien voraus. Schnell folgt dann die Veröffentlichung falscher Infos auf diesen Kanälen.

„Ich kenne keine Statistik über Desinformation gegen Unternehmen, aber wir haben keine signifikante Steigerung von Vorfällen festgestellt“, sagt **Günther Schotten**, Geschäftsführer des ASW Bundesverband (Allianz für Sicherheit in der Wirtschaft). Stärker als im Inland hat die deutsche Wirtschaft damit zum Beispiel in **China** zu kämpfen. „Sie steht dort in Konkurrenz zu einheimischen Unternehmen. Manchmal werden die

Produkte der deutschen Firmen schlecht gemacht, angebliche Gesetzesverstöße angeprangert oder negative Falschinfos über die Unternehmensvertreter gestreut“, berichtet Schotten. Ins Visier der Täter:innen geraten vor allem erfolgreiche Unternehmen, oft aus dem produzierenden Gewerbe und Konsumartikelhersteller.

Die Gefahren der Desinformation haben kürzlich sogar Bundesbankpräsident **Joachim Nagel** veranlasst, eine **Ausweitung der Bankenaufsicht auf soziale Medien** anzuregen. Er warnte davor, dass Falschmeldungen zu einem Bank-Run führen können. Im Fall der kalifornischen Silicon Valley Bank hatten Äußerungen in den sozialen Medien einen Ansturm auf die Bank beschleunigt und weltweit die Sorge vor einer neuen Finanzkrise vergrößert. Nagel warf die Frage auf, ob auch Desinformation so etwas auslösen könnte. „Ich habe neulich mit Interesse von meinem Kollegen aus Südkorea gehört, dass dort eine Task Force der Bankenaufsicht systematisch die sozialen Medien überwacht“, sagte er dem RedaktionsNetzwerk Deutschland (RND) in einem Interview. Diese sehe dann frühzeitig, wenn sich so etwas abzeichne: „Darüber könnten wir in Europa auch nachdenken.“

Stimmungsmache im Netz auf vielen Kanälen

Der Sicherheitsdienstleister Corporate Trust hat öfter mit **Desinformationskampagnen** zu tun. Zwei Beispiele aus seiner Beratungspraxis illustrieren, wie solche Kampagnen ablaufen und wie Opfer darauf reagieren können. Im ersten Fall wurde gegen einen Online-Elektronikhändler aus Berlin Stimmung gemacht. Die Täter:innen behaupteten auf Rezensionsseiten, Twitter und neuen, eigenen Webseiten, die Produkte wären wegen angeblich fehlender Patente unsicher. „Man merkte, es steckte viel Manpower und IT-Expertise hinter der Attacke“, sagt **Sebastian Okada**, Leiter Intelligence & Investigations bei Corporate Trust.

Ein Konkurrent wollte dadurch seiner eigenen Handelsplattform einen Wettbewerbsvorteil verschaffen. „Wir hinterfragten die Nutzer-Accounts und die Anmeldung der Webseiten, auch wenn das durch neue EU-Regeln erschwert worden war. Wir machten auch Foto-Reverse-Suchen und

nutzten Foto-Gesichtserkennung. So konnten wir aufdecken, dass eine **britische Briefkastenfirma vorgeschoben** worden war. Somit war eine Strafanzeige in UK der beste Weg, das Problem zu bekämpfen“, berichtet er.

Im zweiten Fall geriet ein vor 2019 erfolgreicher ukrainischer Generikahersteller ins Visier eines russischen Konkurrenten. Er veröffentlichte falsche Infos auf russischen Facebook-Seiten. „Die ukrainische Firma wollte mit Wirksamkeitsstudien dagegen halten. Das klappte aber nicht“, sagt **Uwe Knebelsberger**, geschäftsführender Gesellschafter von Corporate Trust. Zu viele Bots waren zu bekämpfen. Der finanzielle Schaden belief sich über ein halbes Jahr auf einen siebenstelligen Betrag. Ein Drittel des weltweiten Umsatzes war bedroht. Schließlich äußerten sich immer mehr Gegenstimmen in den sozialen Medien, so dass die Desinformationskampagne an Wirkung verlor.

Technisches Know-how nützlich

Als Täter agieren in Diktaturen wie China oft staatliche Unternehmen, denn sie sind häufig die Konkurrenten der deutschen Firmen. Geheimdienste und die organisierte Kriminalität arbeiten dagegen nach den Erkenntnissen des ASW wenig mit Desinformation. „Ich glaube nicht, dass Desinformationskampagnen aus Deutschland oder dem DACH-Raum heraus erfolgen. Großunternehmen können sich das wegen der Compliance-Vorschriften nicht leisten“, sagt Knebelsberger. Folglich kommen die Täter:innen oft aus Staaten, die solche Regeln nicht kennen. Die beiden Fachmänner von Corporate Trust nennen **Russland, China, Ukraine, Türkei und Vietnam**, aber auch die EU-Staaten **Bulgarien** und **Rumänien**. In einigen dieser Länder ist das IT-Know-how ausgeprägt, was das Steuern von Falschinformationen im Netz erleichtert. „Zum Anonymisieren von Nutzer-Accounts ist IT-Expertise nötig. Neben die Desinformation treten oft ein Know-how-Abfluss durch Cyberangriffe und DDoS-Attacken“, sagt Knebelsberger.

Wie kann man sich gegen die gezielten Falschinformationen schützen? „Unternehmen sollten zunächst einmal **engmaschig die sozialen Medien verfolgen**. Das ist meist die Aufgabe der Kommunikationsabteilungen“,

rät Schotten. Das gilt besonders, wenn es sich um kontroverse Branchen wie Energie und Rüstung handelt. Stößt ein Unternehmen auf Desinformation, so sollte es schnell reagieren, zum Beispiel durch Gegendarstellungen. „Innerhalb von 24 Stunden von den Betreibern sozialer Netze eine Löschung nach dem Netzwerkdurchsetzungsgesetz zu erwirken ist oft schwer“, sagt Schotten. Richten sich die Ansprüche gegen das Ausland, sind die rechtlichen und faktischen Hürden besonders hoch. Aber auch effektiven Rechtsschutz in Deutschland zu erhalten ist oft nicht einfach.

„Man muss es schaffen, dass sich ein Staatsanwalt für die Angelegenheit interessiert. Das ist vor allem für Mittelständler schwierig“, berichtet Knebelsberger. „Wenn Desinformation passiert, sollte man **schnell Profis einschalten**, denn eine Strafanzeige hat tatsächlich nur eine Chance, wenn private Ermittler die Hintergründe der Tat schon aufgeklärt haben“, sagt Okada. Sein Kollege rät zu mehreren Gegenmaßnahmen im Vorfeld. „Ein Baukasten sollte vorhanden sein: Wie reagieren wir? Welche Schritte ergreifen wir? Welche Möglichkeiten und Experten haben wir, um dagegen vorzugehen?" In sozialen Medien ginge es oft um Stunden oder sogar Minuten. Daher sei ein Ablaufplan und eine Checkliste im Rahmen des Krisenmanagements wichtig.