Gefährlichen Gerüchten vorbeugen

Narrative Angriffe laufen über eine längere Zeit und können den Ruf von Logistikunternehmen erheblich schädigen

Von Dunja Koelwel

Für Jörg von der Heydt, Regional Director DACH beim Sicherheitsunternehmen Bitdefender, ist das Spiel mit falschen Informationen ein wichtiger Bestandteil der modernen Kriegsführung: „Experten sprechen von narrativen Angriffen, weil Missverständnisse, Gerüchte und Falschaussagen gestreut werden, um eine Geschichte in die Welt zu setzen und damit Schaden anzurichten."

Christian Scherg, Geschäftsführer der Revolvermänner, einer Agentur, die sich auf den Schutz, die Verteidigung und den Aufbau der Reputation von Personen und Unternehmen im Internet spezialisiert hat, erläutert diese Art von Angriffen näher: „Narrative Angriffe auf große Logistikunternehmen zielen darauf ab, durch falsche Informationen oder irreführende Berichterstattung Zweifel an der Integrität des Unternehmens zu säen. Insbesondere Logistikunternehmen, die in geopolitisch sensiblen Märkten wie Russland oder dem Iran tätig sind, sind Ziel solcher Angriffe."

> Häufig sind Angreifer nicht in Deutschland oder der EU ansässig und daher nur schwer zu belangen.

Der Mechanismus dieser Angriffe läuft laut Scherg oft über verschiedene Kanäle: Vermeintlich seriöse Websites, Blogs oder Social-Media-Kanäle ausländischer Journalisten konstruieren ein Narrativ, also eine Geschichte, die das Unternehmen mit illegalen oder moralisch fragwürdigen Aktivitäten in Verbindung bringt, etwa in Zusammenhang mit der Umgehung von Sanktionen. Insbesondere E-Mail-Anfragen von Pseudo-Journalisten, die Beweise für Verfehlungen präsentieren wollen, gehören zu diesem Repertoire. Ziel ist es, ein diffuses Gefühl des Misstrauens zu erzeugen, das der Reputation des Unternehmens schadet.

Effektiv schützen

Die Angriffe laufen meist über einen längeren Zeitraum. „Im Gegensatz zu direkten Cyberangriffen auf Unternehmen sind narrative Angriffe subtiler und meist schwerer zu identifizieren", erklärt Steffen Klossek, Inhaber der auf Social Media spezialisierten Agentur Brain Interactive. „Bei narrativen Angriffen, insbesondere auf große Logistikdienstleister, zeigt sich oft ein ähnliches Bild: In der Anfangsphase werden Profile in bestimmten Kreisen aufgebaut, eine Zuhörerschaft generiert und Vertrauen geschaffen. Dann werden häppchenweise Fehlinformationen gestreut und mit Suggestivfragen Meinungen in bestimmte Richtungen gelenkt." Der Ton wird rauer, die Emotionen kochen hoch. Spätestens dann ist der Angriff offensichtlich und der Schaden bereits beträchtlich. Häufig zielen die Angriffe auf Kernkompetenzen wie Seefracht, Luftfracht, Landverkehr oder Kontraktlogistik.

Unternehmen sind diesen Praktiken nicht hilflos ausgeliefert, sondern können sich schützen. „Zunächst gilt es, Richtlinien strikt einzuhalten und die Geschäftspraktiken transparent zu halten, um Angriffsflächen zu minimieren", empfiehlt Scherg. Ebenso wichtig sei eine proaktive Krisenkommunikation: Unternehmen sollten Medien und digitale Kanäle permanent beobachten und bei Falschinformationen schnell und transparent reagieren. Parallel dazu sollten präventiv vertrauenswürdige Kommunikationskanäle – dazu gehören auch Social Media – aufgebaut und gepflegt werden, um im Krisenfall sofort die Deutungshoheit auf den Plattformen behaupten zu können.

Cybersicherheitsmaßnahmen schützen vor Datenlecks und Desinformation, während Mitarbeiterschulungen sicherstellen, dass Angriffe frühzeitig erkannt werden. Darüber hinaus sollten rechtliche Schritte in Betracht gezogen werden, um gegen gezielte Verleumdungen vorzugehen und die langfristige Widerstandsfähigkeit des Unternehmens gegen solche Angriffe sicherzustellen. Schließlich ist ein gutes Image in der Öffentlichkeit ein starkes Bollwerk gegen narrative Angriffe. Durch kontinuierliche Öffentlichkeitsarbeit, die Betonung ethischer Geschäftspraktiken und Corporate Social Responsibility (CSR) können Logistikunternehmen ihre Reputation stärken.

Auch eine frühzeitige Positionierung des Unternehmens zu den eigenen Aktivitäten in geopolitisch sensiblen Märkten und Krisenregionen wirkt präventiv. Sie schließt das Informationsvakuum in der Öffentlichkeit, das einen potenziellen Angriffsvektor darstellt. Werden die eigenen Botschaften frühzeitig über vertrauenswürdige Kanäle kommuniziert, erleichtert dies nicht nur die Identifizierung eines Angriffs, sondern schützt auch die eigene Glaubwürdigkeit im Krisenfall.

Schnell Handeln bei Angriff

Wenn Logistiker einen narrativen Angriff bemerken, ist schnelles und strukturiertes Handeln entscheidend. Zunächst sollte der Angriff analysiert werden, um zu verstehen, welche Behauptungen aufgestellt und über welche Kanäle sie verbreitet werden. Parallel dazu sollte ein internes Krisenteam aus Compliance-, PR-, Rechts- und IT-Experten die Situation bewerten und eine einheitliche Kommunikationsstrategie entwickeln.

Eine enge Zusammenarbeit mit vertrauenswürdigen Medien kann helfen, Falschinformationen richtigzustellen. „Es ist wichtig, Beweise wie Screenshots und E-Mails zu sichern, um später fundiert reagieren zu können. Eine auf Fakten basierende öffentliche Stellungnahme sollte zeitnah veröffentlicht werden, um das Vertrauen der Öffentlichkeit zurückzugewinnen", sagt Scherg.

Handelt es sich bei den Vorwürfen um klare Verleumdungen oder falsche Anschuldigungen, sollten rechtliche Schritte wie Unterlassungserklärungen oder Klagen in Erwägung gezogen werden. Häufig sind die Angreifer jedoch nicht in Deutschland oder der Europäischen Union ansässig und daher nur schwer zu belangen. Sollte dies der Fall sein, ist eine Ausweitung der Kommunikationsstrategie auf Plattform- und Suchmaschinenbetreiber zu erwägen, um die Verbreitung von Verleumdungen oder Falschbehauptungen möglichst zu verhindern oder zu minimieren.

Nach einem solchen Vorfall ist es wichtig, die internen Prozesse zu reflektieren und zu verbessern, um für zukünftige Angriffe besser gewappnet zu sein. Anpassungen in den Bereichen Compliance, Krisenkommunikation und IT-Sicherheit können dazu beitragen, die Resilienz des Unternehmens langfristig zu stärken. ***(rok)***