Positionierung gegen Fake News

Der Handlungsspielraum schließt sich schnell

Falsch- und Desinformationen haben längst begonnen, die Welt massiv zu beeinflussen. Und wir stehen erst am Anfang der Entwicklung.

So wird die umfassende Nutzung der sozialen Medien weitergehen und es wird immer schwieriger, die Kontrolle über die Inhalte zu behalten oder diese zumindest im Rahmen allgemeingültiger Werte und Normen zu steuern. Zudem werden die Entwicklungen im Bereich der künstlichen Intelligenz die Problematik weiter verschärfen, zumindest bis es den Regierungen gelingt, allgemeine, weltweite Richtlinien für die Nutzung zu etablieren. Diese Entwicklung kann für die Menschheit zu einer großen Gefahr werden – und zwar für alle Lebensbereiche.

Aus diesem Grund sollten sich Unternehmen und ihre Steuerungs- und Kontrollfunktionen schnell mit konkreten und übergeordneten Fragestellungen rund um das Thema Fake News beschäftigen. Einige davon könnten sein:

- Ist wertebasierte Führung in Zukunft mehr denn je überlebenswichtig oder wird sie zum Auslaufmodell? Welche Rolle spielt in diesem Zusammenhang die Corporate Governance?
- Wie wollen wir mit unseren Kunden umgehen? Sehen wir sie als unsere Partner oder eher als manipulierbare »Cash Cows«, die auch mit falschen Versprechen zu besänftigen sind?
- Welche Produkte bieten wir diesen Kunden an? Ist die Bedürfniserfüllung nach wie vor ein Kriterium für die Entwicklungen von Produkten und Services oder setzen wir auf unwahre Kommunikation und manipulierende Werbemaßnahmen, um ein falsches Werteversprechen zu etablieren? Geht dieser Ansatz dann lange genug gut, bis z.B. der nächste Dopamin-Kick die negativen Erlebnisse/Erinnerungen sowieso auslöscht?
- Wie gehen wir mit Geschäftspartnern und Lieferanten um? Wie können wir eine gemeinsame Basis finden, auch wenn gewisse Werte in anderen Ländern eventuell anders konnotiert sind? Welche Risiken müssen wir zukünftig in diesem Zusammenhang berücksichtigen?
- Welche Quellen und Daten sind vertrauenswürdig; worauf basieren unsere Businesspläne und Geschäftsmodelle?
- Wie geht die Entwicklung der Fake News weiter? Welche neuen Tools und Möglichkeiten beeinflussen künftig das Geschehen?
- Wie stark wollen wir KI und andere technische Möglichkeiten, trotz aller Bedenken, in Managemententscheidungen einbinden? Erlauben wir gar, dass die KI Managementpositionen übernimmt?

Die Beantwortung dieser Fragen wird immer dringlicher, denn der Fortschritt bei der künstlichen Intelligenz und der Werteverfall – besonders in den Demokratien – nimmt stetig zu. Es bleibt nicht viel Zeit, Strategien und Handlungsweisen festzulegen, um diesen Entwicklungen entgegenzusteuern. Lassen Sie uns offen diskutieren, welche Gefahren wir adressieren müssen, aber genauso, welche Chancen sich aus der Diskussion des Umgangs mit Fake News ergeben.

Dieser Beitrag ist ursprünglich erschienen in:
KPMG Audit Committee Quarterly extra (2025)
Herausgeber: Audit Committee Institute e.V. (ACI), abgerufen am: 18.09.2025.

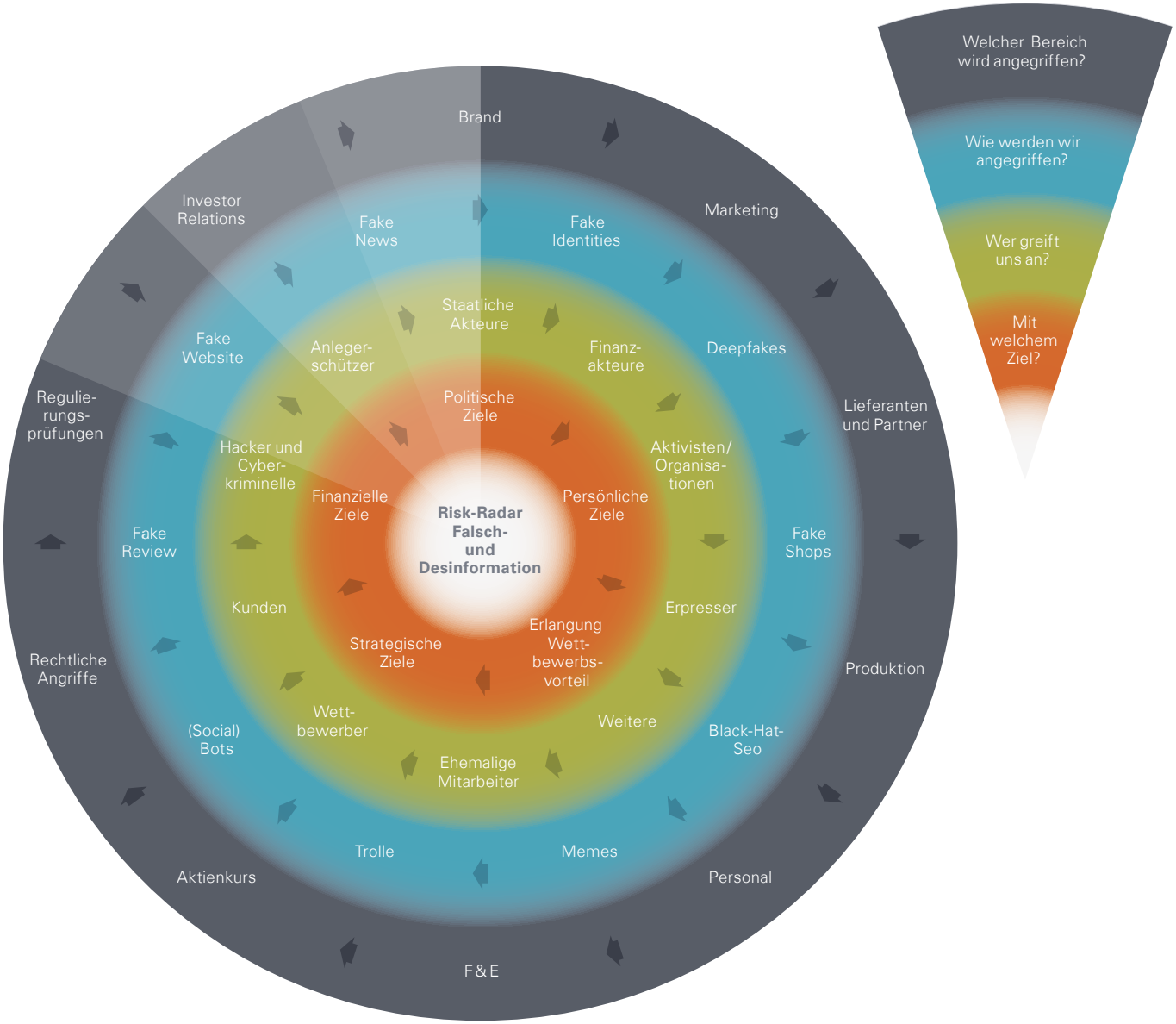
»Fake News Awareness«-Radar für Unternehmen

Fake News können ähnlich wie Cyberattacken nahezu alle Unternehmensbereiche und -verbindungen zu allen in- und externen Stakeholdern betreffen. Im Unternehmen sollte daher präventiv analysiert werden, über welche Handlungsoptionen mögliche Angreifer verfügen und welche Ziele sie verfolgen, um die Abwehr eines potenziellen Angriffs vorzubereiten.

Abhängig von der Art der Bedrohung sollten Unternehmen ihre Prävention und Notfallplanung ausgestalten. In nachfolgendem »Fake News Awareness«-Radar haben wir exemplarisch dargestellt, welche Aspekte in eine solche Analyse einfließen könnten.

»Fake News Awareness«-Radar

(eigene Darstellung von Audit Committee Institute e.V.)



Komponente: Angreifer und Ziele

Der Ausgangspunkt des Fake News-Radars ist die Frage nach möglichen Angreifern und den Zielen, aufgrund derer der Angriff gestartet wird. Diese sind sehr individuell sowie industrie-, unternehmens- oder situationsspezifisch und können daher nicht allgemeingültig in diesem Rahmen erläutert werden.

Vor dem Hintergrund dieser individuellen, unternehmensbezogenen Komponenten sollten dann die beiden weiteren Komponenten des »Wo« (Unternehmensbereich) und des »Wie« (Format) analysiert werden: »Wo und wie werden wir angegriffen?«

Komponente: Unternehmensbereich

In diesem Zusammenhang sollten Unternehmensbereiche oder -prozesse identifiziert werden, die durch Falsch- und Desinformations-Kampagnen betroffen sein können. Einige Beispiele:

Bereich Unternehmensführung und Finanzen

Falsch- und Desinformationen können zu falschen strategischen oder Investitionsentscheidungen führen oder das Vertrauen von (Neu-)Investoren durch gezielte Fake News untergraben. Es ist zudem möglich, dass gezielt platzierte Desinformationen zu verstärkten Prüfungen durch Regulierungsbehörden führen, insbesondere bei angedeuteten rechtswidrigen Aktivitäten. In diesem Zusammenhang sind auch falsche rechtliche Anschuldigungen denkbar, die gerichtlich widerlegt werden müssen, was mit hohem Zeitaufwand verbunden ist. All diese Aspekte können den Unternehmenswert nachhaltig beeinflussen, insbesondere wenn Falschmeldungen über die finanzielle Lage des Unternehmens, über das Ausscheiden von Führungskräften oder über Qualitäts-/Lieferprobleme den Aktienkurs beeinflussen.

Bereich Unternehmenskommunikation

Auch im Bereich der Kommunikation sind Angriffe, beispielsweise auf die Brandattribute eines Unternehmens, möglich. Hier rücken in den letzten Jahren häufig fälschlich negative Berichte über Menschenrechtsverletzungen oder Umweltschutzfragestellungen in den Fokus. Des Weiteren können Fake News im Marketing großen Schaden anrichten, wenn beispielsweise eine Produktaussage angegriffen wird oder ein gewähltes Kampagnengesicht in den negativen Fokus gerät. Fehlerhafte Meldungen in der Presse, etwa zu Managementwechseln, können ebenfalls negative Auswirkungen haben.

Grundsätzlich können alle Bereiche eines Unternehmens gefährdet sein. Sei es durch gestreute Falschinformationen zu Sicherheitsbedenken von Produktionsanlagen und -prozessen, Falschinformation über den Entwicklungsstand von Innovationen, Desinformationen zum Rückgang der Umsatzzahlen und zu finanziellen Einbußen oder durch falsche Informationen im Zusammenhang mit dem Umgang mit Mitarbeitenden und Unternehmenswerten, was die Mitarbeitersuche und Neueinstellungen erschwert. Aber auch im Einkauf und Vertrieb können Desinformationen über Geschäftspraktiken oder den Umgang mit Partnern zu Problemen führen. Die Risikobereiche sind für jedes Unternehmen individuell und sollten im Rahmen der Prävention analysiert und diskutiert werden.

Neben diesen beispielhaften Aspekten, die das Unternehmen unmittelbar betreffen, liegen auch im privaten Bereich zusätzliche Risiken. Jede Person im Unternehmen – und natürlich insbesondere das nach außen exponierte Management oder der Aufsichtsrat – kann im Rahmen von Fake News-Kampagnen zum Risiko für das gesamte Unternehmen werden. Hier ist es beispielsweise vorstellbar, dass persönliche oder politische Vorlieben für Kampagnen gegen das Unternehmen genutzt werden. Des Weiteren kann die kritische Darstellung von Thematiken (wie Unabhängigkeit) rund um den Aufsichtsrat leicht Auswirkungen auf das Unternehmen haben. Werden solche Informationen gezielt falsch kommuniziert, kann einem Unternehmen ein extremer Reputationsschaden entstehen, obwohl keine Produkte/Prozesse im Unternehmen direkt betroffen sind.

Komponente: Formate

Auf einer weiteren Ebene des »Fake News Awareness«-Radars geht es um die Formate, die für einen Angriff genutzt werden können. Einige Angreifer legen ihren Schwerpunkt auf Social Media (soziale Netzwerke und Messenger), andere nutzen alle digitalen Kanäle. Besonders erfolgreich sind meistens die Angriffe, denen eine umfassende, koordinierte Kampagne zugrunde liegt. Diese Kampagnen können gezielt Informationsdefizite bei den Empfängern ausnutzen oder bestimmte Aspekte falsch verstärken.

Nachstehend einige häufig genutzte Angriffsformate:

- Fake Identities: Darunter versteht man die Nutzung von erfundenen oder gestohlenen Daten, Dokumenten oder Online-Profilen, um einen bestimmten Absender vorzutäuschen (z.B. CEO-Fraud). Inzwischen werden in diesem Zusammenhang auch umfassend Deep Fakes eingesetzt, z.B. in Videos, die den CEO oder sogar ganze Gruppen von Führungskräften real nachbilden.

- Fake Shops: Diese Formate werden eingesetzt, um Kunden durch besonders verlockende Angebote zum Kauf zu verführen, z.B. Markenartikel zu sehr günstigen Preisen. Diese Angebote werden oftmals in Social-Media-Apps oder auf falschen Websites platziert; sie können dem Ruf des Unternehmens massiv schaden, wenn Produkte falsch bepreist angeboten und dann nicht geliefert werden können.

- Fake Websites: Hierbei handelt es sich um falsche, nachgebaute Unternehmenswebseiten mit in der Regel für das Unternehmen schädlichem Inhalt, die oft unbemerkt durch eine URL-Umleitung angesteuert werden.

- Fake Reviews: Fehlerhafte und unwahre Informationen im Zusammenhang mit der Bewertung von Services und Produkten. Häufig eingesetzt bei technischen Produkten der Konsumgüterindustrie (z.B. elektronischen Geräten) und Hotelbewertungen.

Die folgenden Formate werden besonders in sozialen Netzwerken und Messengern genutzt:

- Deepfakes (Ton, Bild, Video): Mithilfe von KI ist es immer einfacher möglich, reale Personen in einer falschen Umgebung und mit falschen, nicht getätigten Aussagen darzustellen. Inzwischen kann das Gesicht oder der gesamte Körper realitätsnah in jedes Video geschnitten werden (z.B. bei gefälschten Pornovideos), die Lippensynchronisation kann an jeden Text angepasst werden und Stimmen können perfekt imitiert werden. Darüber hinaus ist es möglich, virtuelle Gesichter oder ganze Personen zu erstellen, die absolut real erscheinen.

- Memes: Memes sind in der Regel Bilder, Videos oder Texte mit humorvollem oder satirischem Inhalt, die überwiegend im Internet und in Social Media verbreitet werden. Memes können einfach individuell angepasst und millionenfach geteilt werden – wodurch sie eine große Wirkung bei der Verbreitung von Fake News erzielen können.

- Social Bots: Social Bots sind gezielt programmierte Tools, die eingesetzt werden, um Klicks zu generieren oder Meinungen zu manipulieren. Social Bots sind die Weiterentwicklung des »Troll«-Konzepts in digitaler Massenform. Da sie wie menschliche Nutzer handeln und in Echtzeit auf Debatten reagieren, können sie massenhafte Zustimmung oder Ablehnung simulieren und so gravierenden Einfluss auf jede Diskussion nehmen.

Das Fake News-Radar kann für Unternehmen eine erste Möglichkeit sein, eine Angreifbarkeit durch Falsch- und Desinformationen zu prognostizieren und eine längerfristige Strategie zu entwickeln, die Werte und Verhaltensnormen auch mit Blick auf die Zukunft prägt.

Kontakt

Manuela Mayer
Head of Board Services

M +43 664 816 1162
manuelamayer@kpmg.at

kpmg.at