ServiceCenter Verbände I Kommunikation und Öffentlichkeitsarbeit

Sicherer Umgang mit Desinformation

vbw

Leitfaden
Stand: Januar 2026

Die bayerische Wirtschaft

Vorwort

Desinformation als Risiko für die Wirtschaft

Desinformation ist zu einem ernstzunehmenden Risiko für Unternehmen, Verbände und wirtschaftspolitische Entscheidungsprozesse geworden. Gezielt verbreitete Falschinformationen können erhebliche Reputations- und Vermögensschäden verursachen, Vertrauen untergraben und Unsicherheit bei Mitarbeitenden, Kunden und der Öffentlichkeit auslösen. Für die bayerische Wirtschaft ist der souveräne Umgang mit Desinformation damit ein zentraler Faktor für Stabilität und Wettbewerbsfähigkeit.

Die zunehmende Digitalisierung der öffentlichen Kommunikation sowie der Einsatz Künstlicher Intelligenz erleichtern die schnelle, skalierbare Verbreitung manipulativer Inhalte. Gleichzeitig sind Unternehmen und Verbände auf faktenbasierte, transparente Kommunikation angewiesen. Umso wichtiger ist es, über klare Strukturen, abgestimmte Prozesse und Handlungssicherheit im Umgang mit Desinformationsfällen zu verfügen.

Unser Ziel ist es, die Resilienz der bayerischen Wirtschaft zu stärken, Handlungssicherheit zu schaffen und Vertrauen in eine verlässliche, faktenbasierte Kommunikation zu sichern. Ein wesentlicher Baustein ist das Engagement der vbw in der Bayern-Allianz gegen Desinformation[1], in der Wirtschaft, Staat, Wissenschaft, Medien und Zivilgesellschaft gemeinsam daran arbeiten, Desinformation einzudämmen und die Informations- und Medienkompetenz zu stärken.

Der vorliegende Leitfaden bietet praxisnahe Orientierung für Kommunikationsverantwortliche in Unternehmen und Verbänden. Er zeigt auf, wie Desinformationsfälle frühzeitig erkannt, realistisch bewertet und strukturiert bearbeitet werden können. Ziel ist es, die Handlungsfähigkeit der bayerischen Wirtschaft zu stärken – präventiv wie reaktiv. Wer vorbereitet ist, klare Prozesse etabliert und seine Kommunikation entlang verlässlicher „langer Linien“ ausrichtet, reduziert nicht nur Risiken, sondern stärkt auch Vertrauen und Glaubwürdigkeit.

Bertram Brossardt
Januar 2026

[1] Mehr dazu: https://www.stmd.bayern.de/themen/bayern-allianz-desinformation/

Inhalt

1 Einleitung

Relevanz von Desinformation für die Wirtschaft im Jahr 2026

Desinformation – also gezielt verbreitete Falschinformationen – hat sich bis 2026 zu einem ernstzunehmenden Risiko für Unternehmen und Verbände entwickelt. Die zunehmende Bedeutung von Social-Media-Kommunikation im Verbands- und Unternehmenskontext sowie die breite Verfügbarkeit generativer KI-Modelle haben dazu geführt, dass Desinformation gegen wirtschaftliche Akteure leichter, zielgenauer und skalierbarer verbreitet werden kann. Die Folgen reichen von Gewinneinbrüchen und Reputationsschäden über gestörte Stakeholderbeziehungen und regulatorische Herausforderungen bis hin zur Erosion interner Verbands- und Unternehmensdynamiken.

Der wirtschaftliche Schaden durch Desinformation bzw. „Fake News“ wurde bereits 2019 von der University of Baltimore auf rund 78 Milliarden US-Dollar pro Jahr geschätzt.[2] Der Global Risks Report 2024 und der Global Risks Report 2025 des Weltwirtschaftsforums stufen Desinformation zudem zwei Jahre in Folge als größtes kurzfristiges globales Risiko ein.[3][4] Eine Studie der Bertelsmann Stiftung aus dem Februar 2024 zeigt darüber hinaus, dass 84 Prozent der Menschen in Deutschland vorsätzlich verbreitete Falschinformationen im Internet als großes oder sehr großes gesellschaftliches Problem wahrnehmen.[5] Damit wird deutlich, dass Verbände und Unternehmen nicht nur zunehmend im Fadenkreuz von Desinformation stehen, sondern zugleich auch eine gesellschaftliche Verantwortung an sie herangetragen wird.

Gleichzeitig haben faktenbasierte Akteure einen strukturellen Nachteil: Während schädliche Akteure widersprüchliche Narrative in hoher Frequenz und emotional zugespitzt verbreiten können, sind Unternehmen und Verbände an hohe Standards der Informationsqualität gebunden. Umso wichtiger ist ein klarer Handlungsrahmen, der hilft, Desinformationsfälle frühzeitig zu erkennen, realistisch einzuordnen und strukturiert zu bearbeiten.

Dieser Leitfaden soll Kommunikationsverantwortliche der bayerischen Wirtschaft dabei unterstützen, Handlungssicherheit im Umgang mit Desinformation zu gewinnen. Er bietet eine verlässliche, aktuelle und praxisnahe Systematik, die von Verbänden und Unternehmen unkompliziert angewendet werden kann.

---

[2] University of Baltimore / CHEQ. (2019): *The Economic Cost of Fake News*. University of Baltimore / CHEQ. https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf

[3] Weltwirtschaftsforum. (2024): *Global Risks Report 2024 – Presseinformation (DE)*. Weltwirtschaftsforum. https://www3.weforum.org/docs/WEF_GRR24_Press%20release_DE.pd

[4] Weltwirtschaftsforum. (2025): *Global Risks Report 2025: Conflict, environment and disinformation top threats*. Weltwirtschaftsforum. https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/

[5] Berger, C. / Unzicker, K. (2024): *Große Mehrheit erkennt in Desinformation eine Gefahr für Demokratie und Zusammenhalt*. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2024/februar/grosse-mehrheit-erkennt-in-desinformation-eine-gefahr-fuer-demokratie-und-zusammenhalt

2 Typische Falltypen aus der Verbände- und Unternehmenspraxis

Bandbreite relevanter Angriffsarten, die über strategisch geplante Desinformationskampagnen hinausgehen

Gefälschte Social-Media-Profile (Impersonation):

Eine der am häufigsten auftretenden Formen der Informationsmanipulation ist die Erstellung sogenannter „Doppelgänger"-Profile oder -Webseiten. Angreifer legen in sozialen Netzwerken gefälschte Accounts an, um sich als Verband, Unternehmen oder Mitarbeitende der jeweiligen Organisation auszugeben. So war unter anderem die Vereinigung der Bayerischen Wirtschaft im Sommer 2025 betroffen: Ein gleichnamiges Fake-Profil verschickte gefälschte Nachrichten und kontaktierte über Facebook-Konten gezielt Personen aus der Followerschaft der Originalprofile. Die Empfänger wurden aufgefordert, einer WhatsApp-Gruppe beizutreten und persönliche Daten zu übermitteln, woraufhin sie in einen Finanz-Scam hineingezogen werden sollten.

Abbildung 1

Frühzeitige öffentliche Klarstellung der vbw auf Instagram bei Impersonation

Vereinigung der Bayerischen Wirtschaft e. V. (vbw). Warnhinweis zu Fake-Profilen im Umlauf. 2025. https://www.instagram.com/p/DM94t9gNOTD/.

Der wahrscheinlich bekannteste Fall ist der „Eli Lilly“-Vorfall im Jahr 2022, bei dem ein gefälschtes Twitter-Profil des Pharmaunternehmens die angebliche kostenfreie Abgabe von Insulin ankündigte und innerhalb weniger Stunden zu erheblichen Kursverlusten und massiver öffentlicher Verwirrung führte.[6]

Diese Beispiele verdeutlichen, dass es sich bei derartigen Angriffen nicht immer um explizite Narrative gegen eine Organisation handeln muss. Häufig liegt der Fokus vielmehr auf finanziellen Motiven, bei denen Identitätsdiebstahl gezielt zur Anbahnung von Betrugsmodellen genutzt wird.

Deepfakes und manipulierte Medien:

Insbesondere mit Blick auf die Simulation real existierender Personen für Desinformationszwecke haben Deepfake-Videos und -Audios in den vergangenen Jahren erheblich an Relevanz gewonnen. Durch generative KI können realen Personen – etwa einer oder einem CEO – deutlich leichter täuschend echte Aussagen zugeschrieben werden, die sie nie getroffen haben. Solche Inhalte dienen dazu, Verwirrung zu stiften, die Glaubwürdigkeit einer Organisation zu beschädigen oder in Social-Engineering-Kontexten interne Daten und Zugänge abzugreifen.

In diesem Kontext hat auch das Phänomen sogenannter „AI slop“ deutlich zugenommen, also massenhaft generierte, qualitativ minderwertige, aber optisch oder sprachlich überzeugend wirkende KI-Inhalte, die ohne klare Urheberschaft oder Einordnung verbreitet werden. Solche Inhalte verwischen die Grenzen zwischen authentischem und künstlich erzeugtem Material zunehmend und erhöhen das Grundrauschen, in dem gezielte Fälschungen wie Deepfakes leichter untergehen oder ungeprüft weiterverbreitet werden. Für Unternehmen erschwert dies die zeitnahe Identifikation manipulierter Inhalte und erhöht das Risiko, dass Desinformation schnell an Fahrt gewinnt, bevor Gegenmaßnahmen greifen.
Ein aktuelles Deepfake-Beispiel aus dem Jahr 2025 ist der Fall um Bayer-CEO Bill Anderson: Ein KI-generiertes Video zeigte ihn vermeintlich in einer australischen TV-Sendung, in der er für ein neuartiges Abnehmpräparat warb, das vollständig erfunden war. Der Konzern reagierte schnell, ordnete den Deepfake öffentlich ein und baute als Reaktion eine interne Deepfake-Taskforce auf.[7]

Der Fall verdeutlicht, wie glaubwürdig und professionell solche Manipulationen inzwischen produziert werden können und welche Bedeutung vorbereitete Reaktionsprozesse für Verbände und Unternehmen haben.

Manipulative Narrative und verzerrte Behauptungen:

Manipulative Erzählungen über Organisationen oder Einzelpersonen gehören zu den wirkungsvollsten Formen reputationsbezogener Desinformation, insbesondere dort, wo

---

[6] Spiegel Online. (2022): *Aktienkurs von Insulinhersteller fällt nach Fake-Tweet*. Spiegel Online. https://www.spiegel.de/wirtschaft/unternehmen/twitter-chaos-aktienkurs-von-insulinhersteller-faellt-nach-fake-tweet-a-cd2eebad-54aa-4c33-81d9-6b37c78dd733
[7] Dunkel, M. (2025): *KI-Betrug: Bayer-Chef Bill Anderson wurde Deepfake-Opfer*. Capital. https://www.capital.de/wirtschaft-politik/ki-betrug--bayer-chef-bill-anderson-wurde-deepfake-opfer-35486154.html

wirtschaftliche und gesellschaftliche Verantwortung miteinander verwoben sind. Diese Form der Informationsmanipulation zielt darauf ab, über in sich konsistente falsche Botschaften einen Vertrauensverlust zu erzeugen, maximale Verwirrung durch widersprüchliche Narrative hervorzurufen oder durch den gezielten Einbezug von Influencern der Falschinformation zusätzliche Glaubwürdigkeit zu verleihen.

Inhaltlich bedienen solche Narrative eine breite Schnittmenge möglicher Angriffspunkte: vermeintlich negative Unternehmensentwicklungen wie Massenentlassungen oder problematische Geschäftspraktiken, angebliche Verstöße gegen Standards – etwa im ESG-Kontext –, aber auch konstruierte Anschuldigungen zum Verhalten oder Privatleben einzelner Führungskräfte. Dabei reicht das Spektrum von vollständig erfundenen Vorwürfen und Verschwörungserzählungen bis hin zu realen Entwicklungen, die gezielt verzerrt, aus dem Kontext gerissen oder manipulativ überhöht dargestellt werden.

So waren beispielsweise im Rahmen der Gasmangellage nach dem Beginn des russischen Angriffskrieg auf die Ukraine ab dem Jahr 2022 insbesondere energieintensive deutsche Unternehmen verstärkt Ziel entsprechender Desinformation. In mehreren Fällen kursierten Behauptungen über angebliche Werksschließungen oder Produktionsstopps, etwa bei BASF, Siemens oder Volkswagen, die sich in diesem Ausmaß als vollständig erfunden erwiesen und dazu dienten, bestehende Unsicherheiten weiter zu verstärken.[8]

Solche Narrative entfalten ihre Wirkung, insbesondere dadurch, dass sie genau an diese bestehenden Unsicherheiten, Vorurteile oder gesellschaftlichen Spannungen anknüpfen. Dadurch wirken sie trotz fehlender faktischer Grundlage häufig plausibel und können erheblichen Schaden verursachen.

Gefälschte Dokumente und Fake-Mitteilungen:

Meist als Instrument im Rahmen größer angelegter Kampagnen werden professionell gefälschte Briefe, Pressemitteilungen oder interne Memos eingesetzt. Sie erwecken den Anschein offizieller, glaubwürdiger Informationen und können dadurch erhebliche negative Konsequenzen hervorrufen. Angreifer nutzen dabei Logos, Layouts und Sprachstile der betroffenen Organisationen, um Echtheit vorzutäuschen. Ein Beispiel aus dem Jahr 2024 zeigt, wie wirkungsvoll solche Manipulationen sein können: Im Februar des Jahres verbreitete ein X-Account gefälschte Pressemitteilungen, die täuschend echt im Format der Europäischen Kommission und des Weißen Hauses gestaltet waren. Die Mitteilungen suggerierten eine politische Kehrtwende der EU und der USA in den Verhandlungen zum WHO-Pandemievertrag – einem Abkommen, das globale Regeln für Lieferketten, Produktionskapazitäten und die Verteilung medizinischer Güter festlegen sollte und damit für zahlreiche Unternehmen direkte regulatorische Relevanz besitzt.[9]

---

[8] Echtermann, A. (2022): *Fake-Kampagne: Werke von BASF, Siemens oder VW werden nicht wegen Energiekrise geschlossen*. Correctiv. https://correctiv.org/faktencheck/2022/12/08/fake-kampagne-werke-von-basf-siemens-oder-vw-werden-nicht-wegen-energiekrise-geschlossen/

[9] Wheaton, S. (2024): *When civil society resorts to fake news*. Politico Europe. https://www.politico.eu/newsletter/politico-eu-influence/when-civil-society-resorts-to-fake-news-2/

Solche falschen Mitteilungen nutzen gezielt das Vertrauen der Öffentlichkeit in visuelle und formale Echtheitsmerkmale, um Medien, Stakeholder und politische Entscheidungsprozesse zu beeinflussen.

Koordinierte Troll- und Bot-Kampagnen:

Falschinformationen werden häufig durch automatisierte Social Bots oder koordinierte Trollnetzwerke verbreitet. Social Bots sind automatisierte Accounts, die Inhalte in hoher Frequenz posten, teilen oder liken, während Trolle echte Personen sind, die bewusst polarisierende oder irreführende Inhalte verbreiten. Beide Mechanismen erzeugen künstlich den Eindruck hoher Resonanz und gesellschaftlicher Relevanz, wodurch Falschinformationen schneller Reichweite erzielen und glaubwürdiger wirken.

Besonders deutlich wurde dies im Bankensektor während des Zusammenbruchs der Silicon Valley Bank im Jahr 2023: In den Tagen vor und nach der Insolvenz verbreiteten sich auf Social Media massenhaft irreführende oder alarmistische Inhalte, darunter wiederholte Narrative zu angeblichen politischen Ursachen oder bevorstehenden weiteren Bankenzusammenbrüchen, die durch hochfrequente Accounts und orchestrierte Online-Communities verstärkt wurden.[10] Diese Dynamik trug zur Verunsicherung von Kunden bei und verschärfte die Informationslage in einer ohnehin volatilen Krisensituation.

Manipulierte Bewertungen und KI-Modelle:

Ein subtilerer, aber häufig wirkungsvoller Angriffsvektor sind gefälschte Kundenrezensionen oder manipulierte Arbeitgeberbewertungen. Diese zielen darauf ab, das Vertrauen von Verbraucher*innen, Bewerber*innen oder Geschäftspartnern zu untergraben. Gefälschte 1-Sterne-Bewertungen oder frei erfundene Erfahrungsberichte können so das Kundenvertrauen und die Arbeitgebermarke erheblich beschädigen. Parallel dazu ist in den vergangenen Jahren ein weiteres Muster der Informationsmanipulation sichtbar geworden: Organisierte Akteure versuchen gezielt, Suchmaschinen oder KI-Modelle durch die massenhafte Verbreitung bestimmter Inhalte zu beeinflussen. Solche Aktivitäten dienen nicht der Bewertung einzelner Unternehmen oder Produkte, sondern verfolgen politische oder gesellschaftliche Narrative. Ein dokumentiertes Beispiel hierfür ist ein russisches Online-Netzwerk, das große Mengen propagandistischer Texte in das offene Web einspeiste, um Sprachmodelle und deren Antworten zu beeinflussen.[11]

Die beschriebenen Fälle zeigen, dass Desinformation branchenübergreifend jedes Unternehmen und jeden Verband treffen kann. Die Motive reichen von finanziellen und politischen Interessen bis hin zu Sabotage oder ideologischen Zielen.

---

[10] Alethea. (2025): *When crisis strikes, disinformation thrives*. Alethea. https://alethea.com/insights/when-crisis-strikes-disinformation-thrives

[11] Tagesspiegel. (2025): *LLM-Grooming-Methode: Russland manipuliert offenbar westliche Chatbots für seine Propaganda*. Der Tagesspiegel. https://www.tagesspiegel.de/internationales/llm-grooming-methode-russland-manipuliert-offenbar-westliche-chatbots-fur-seine-propaganda-13370401.html

3 Schritt-für-Schritt-Reaktionsleitfäden

Strukturierter Umgang mit Desinformation – von der frühzeitigen Identifikation bis zur Nachbereitung

3.1 Frühzeitige Identifikation von Desinformationsfällen

Während viele Krisen, die für einen Verband oder ein Unternehmen relevant werden können, sich über Tage oder sogar Wochen abzeichnen, entstehen Desinformationskampagnen und einzelne Angriffe der Informationsmanipulation häufig innerhalb weniger Stunden. Für ein verlässliches internes Identifikationssystem braucht es daher das Zusammenspiel aus menschlichem Wissen und entsprechenden Kompetenzen, technologischen Hilfsmitteln sowie funktionierenden internen Melde- und Bewertungsprozessen.

3.1.1 Warnsignale erkennen

Die frühzeitige Identifikation potenzieller Desinformation gelingt am zuverlässigsten, wenn alle Personen mit Außenkontakt – sei es analog oder digital – nicht nur grundsätzlich wachsam sind, sondern gleichzeitig so geschult werden, dass sie typische Warnsignale frühzeitig erkennen können. Dazu gehört, Medien- und Informationskompetenz ebenso wie Cybersecurity- und Datenschutzschulungen aufzubauen. Mitarbeitende sollten befähigt werden, echte von manipulierten Inhalten besser zu unterscheiden, typische Merkmale manipulativer Beiträge zu erkennen (z. B. extreme Emotionalisierung, fehlende seriöse Quellen, unklare oder ungewöhnliche Absender) und aufmerksam für Hinweise auf Impersonation oder unplausible Kommunikationsmuster zu bleiben.

Die in Kapitel 2 beschriebenen Falltypen ermöglichen es Mitarbeitenden in Verbänden und Unternehmen, gezielte Fragen zu formulieren, mit denen sie bereits in der frühen Phase eines potenziellen Vorfalls zentrale Warnsignale erkennen können.

Gefälschte Social-Media-Profile (Impersonation):

Wirkt das Profil, das uns kontaktiert oder erwähnt, echt und konsistent mit dem offiziellen Auftritt der Organisation oder Person?

Deepfakes und manipulierte Medien:

Stimmen Erscheinungsbild, Stimme und Kontext des Materials mit dem üblichen Auftreten der realen Person überein?

Manipulative Narrative und verzerrte Behauptungen:

Handelt es sich um eine plötzlich auftretende Erzählung, die sich auf eine unklare oder nicht überprüfbare Quellenlage stützt und gleichzeitig auf vielen Kanälen in ähnlicher Form verbreitet wird?

Gefälschte Dokumente und Fake-Mitteilungen:

Ist das Dokument in Format, Sprache und Absenderangaben konsistent mit bisherigen offiziellen Mitteilungen?

Koordinierte Troll- und Bot-Kampagnen:

Entspricht das Interaktionsverhalten einem organischen Verlauf oder wirkt es künstlich synchronisiert?

Manipulierte Bewertungen und gezielte Einflussnahme auf KI-Modelle:

Entsteht plötzlich ein Muster sich wiederholender Formulierungen oder Bewertungen, das nicht zu realem Kunden- oder Stakeholderverhalten passt?

3.1.2 Monitoring-Quellen und -Werkzeuge

Neben der individuellen Aufmerksamkeit von Mitarbeitenden benötigt eine wirksame Früherkennung von Desinformation auch ein strukturiertes Monitoring. Ziel ist es, relevante Signale systematisch zu erfassen. Je schneller neue Narrative, Auffälligkeiten in Interaktionsmustern oder untypische Account-Aktivitäten erkannt werden, desto früher kann eine angemessene interne Abstimmung beginnen.

Frühe Hinweise auf Desinformationskampagnen lassen sich aus zwei Arten von Quellen ableiten, die je nach Falltyp miteinander überlappen können:

Externe Informationsquellen:

Dazu gehören Social-Media-Plattformen, Nachrichtenmedien, Foren, Kommentarspalten und offene Diskussionsräume. Hier entstehen Desinformationsdynamiken häufig zuerst, sei es durch neu angelegte Profile, abrupt aufkommende Narrative oder auffällige Interaktionsmuster. Auch geschlossene Räume wie Messenger-Gruppen oder private Facebook-Communities können relevante Hinweise liefern, sofern Mitarbeitende oder weitere Mitglieder problematische Inhalte melden.

Interne Informationsquellen:

Frühwarnsignale entstehen häufig auch innerhalb der Organisation, z. B. durch Rückmeldungen aus Kundenkontakt, Mitgliedsverbänden, Service-Hotlines, HR oder Beschwerdemanagement.

Um insbesondere die Signale in externen Informationsquellen effizient erkennen zu können, sind Monitoring-Tools hilfreich, insbesondere wenn bereits Werkzeuge im Unternehmen vorhanden sind, die lediglich an die Anforderungen von Desinformation angepasst werden müssen. Dazu zählen Social-Media-Monitoring-Tools, Medien- und Policymonitorings sowie Keyword-Alerts oder Reputationsmanagement-Tools. Bevor also die Parameter für die Identifikation genutzt werden, sollte geprüft werden, welches Monitoring-Tool die Anforderungen des Verbandes oder Unternehmens am besten erfüllt: etwa hinsichtlich

Plattformabdeckung, Echtzeitfähigkeit, Erkennungslogiken für ungewöhnliche Muster oder Möglichkeiten zur Integration in bestehende Systeme.

Die Einrichtung eines derartigen Monitorings zur Identifikation von Desinformation lässt sich grob anhand folgender Schritte orientieren:

1. Festlegung relevanter Suchbegriffe und Beobachtungsfelder:
   Im Tool werden Verbands- bzw. Unternehmensnamen, Produktnamen, Führungspersonen, Standortbezüge sowie häufig genutzte Falschschreibweisen oder abwertende Begriffe hinterlegt. Ergänzend empfiehlt sich eine „Blacklist“ potenzieller Narrative, die im Branchenkontext eine Rolle spielen.
2. Einrichtung regelbasierter Alerts:
   Alerts werden so konfiguriert, dass sie ausgelöst werden, wenn bestimmte Schwellenwerte überschritten werden, wie etwa ungewöhnliche Anstiege im Erwähnungsvolumen, neue Schlagworte, regionale Häufungen oder ungewöhnliche Quellen.
3. Prüfung der auffälligen Treffer:
   Bei ausgelösten Alerts wird zunächst geprüft, welche Accounts beteiligt sind, ob erkennbare Muster vorliegen und ob Aussagen auf Primärquellen zurückgeführt werden können. Gleichzeitig wird bewertet, ob es sich um ein organisches Diskussionsthema oder um einen potenziell orchestrierten Vorgang handelt.
4. Analyse der Dynamik und Verbreitungsmuster:
   Tauchen Inhalte gleichzeitig auf mehreren Plattformen auf? Wird der Wortlaut kopiert? Handelt es sich um neu erstellte Accounts? Solche Muster helfen bei der Einordnung der möglichen Relevanz.
5. Verknüpfung mit internen Meldungen (siehe Abschnitt 3.1.3):
   Auffälligkeiten aus dem Monitoring sollten mit internen Hinweisen abgeglichen werden (z. B. verunsicherte Anrufe, Beschwerden, ungewöhnliche Presseanfragen), um ein vollständigeres Lagebild zu erhalten.

Wichtig ist, dass Monitoring-Ergebnisse regelmäßig geprüft und intern kommuniziert werden, idealerweise in kurzen Lagehinweisen oder in einem festen täglichen bzw. wöchentlichen Rhythmus.

3.1.3 Interne Melde- und Bewertungsprozesse

Damit Hinweise schnell zusammengeführt und bewertet werden können, braucht es in Verbänden und Unternehmen standardisierte Meldewege, klare Zuständigkeiten und erste Prüfmechanismen für Desinformationsfälle.

Niedrigschwellige Meldestrukturen:

Alle Mitarbeitenden sollten wissen, an welche zentrale Stelle sie verdächtige Inhalte oder ungewöhnliche Interaktionen weiterleiten können. Eine einfache Anlaufstelle – etwa eine gemeinsame Funktionsadresse, ein internes Formular oder ein definierter Kommunikationskanal – senkt die Hemmschwelle und sorgt dafür, dass Hinweise nicht verloren gehen.

Zentrale Erstbewertung:

Die eingehenden Hinweise sollten in einer ersten, strukturierten Kurzbewertung geprüft werden. Dabei geht es nicht um eine vollständige Analyse, sondern um eine schnelle Einordnung:

- Handelt es sich um ein Einzelfragment oder sehen wir erste Muster?
- Liegt ein Bezug zu den in Kapitel 2 beschriebenen Falltypen nahe?
- Sind technische oder organisatorische Komponenten betroffen (z. B. mögliche Impersonation)?
- Gibt es erste Anzeichen für Verbreitungsdynamik?

Diese Einschätzung sollte unkompliziert machbar sein, denn eine grobe Zuordnung in niedriges, mittleres oder erhöhtes Risiko genügt an dieser Stelle bereits, um die nächsten Schritte zu steuern, ohne Entscheidungswege zu verlangsamen. Die Erstbewertung kann in der Kommunikations- oder Public-Affairs-Abteilung, in einem kleinen Kernteam aus beiden, oder – je nach Organisationsgröße – in einer definierten Monitoring-Einheit erfolgen.

Dokumentation und Informationsbündelung:

Um die spätere Analyse zu erleichtern, sollten relevante Informationen standardisiert erfasst werden: Plattform, Account, Zeitpunkt, Art des Inhalts, Screenshots bzw. Archivlinks und eine erste Einschätzung. So entsteht ein konsistentes Bild, das unabhängig von Personen nachvollzogen werden kann.

Schnelle interne Abstimmung:

Stellt die Erstbewertung einen möglichen Desinformationsfall in Aussicht, sollte zeitnah eine kurze interne Abstimmung erfolgen, idealerweise mit Kommunikation, Public Affairs (PA), Recht, Cybersecurity / IT und bei Bedarf Geschäftsleitung. Diese Abstimmung dient nicht der vollständigen Bewertung, sondern der Formulierung einer ersten gemeinsamen Lageeinschätzung:

- Ist die Situation beobachtungsbedürftig?
- Muss das Monitoring intensiviert werden?
- Sind Schutzmaßnahmen oder vorbereitende Kommunikationsschritte sinnvoll?

Wenn interne Hinweise und Erstprüfung ein stimmiges Bild ergeben, wird der Fall in den formalen Risikoabschätzungsprozess übergeben, der im nächsten Kapitel dargelegt wird.

3.2 Risikoabschätzung

Nachdem erste Warnsignale erkannt und intern geprüft wurden, folgt die strukturierte Risikoabschätzung. Sie dient dazu, die Bedeutung eines Vorfalls realistisch einzuordnen und zu entscheiden, ob – und wenn ja welche – Form der Reaktion erforderlich ist. Ziel ist es, aus einzelnen Fragmenten und ersten Hinweisen ein konsistentes Lagebild abzuleiten, das sowohl die aktuelle Dynamik als auch das potenzielle Risiko berücksichtigt.

Die Bewertung orientiert sich an fünf Kernkriterien, die unabhängig davon angewendet werden können, ob es sich um eine breit angelegte Kampagne oder einen isolierten, aber wirkungsvollen Manipulationsversuch handelt. Verbände und Unternehmen können daraus ein einfaches Scoring-System entwickeln, indem jedes Kriterium auf einer Skala von 1 (sehr niedrig) bis 5 (sehr hoch) bewertet wird. Die Summe ergibt eine Risikoeinstufung, die als Grundlage für die Auswahl geeigneter Reaktionsmaßnahmen dient.

Tabelle 1
Risikomatrix mit Scoring-System

Kriterium	1 = Sehr niedrig	3 = Mittel	5 = sehr hoch
Reichweite		x	
Medienerwähnungen	x		
Absender			x
Gefahr		x	
Dringlichkeit	x		

Reichweite: Wie schnell verbreitet sich der Inhalt?

Hier wird bewertet, ob der Vorfall nur punktuell auftritt oder bereits erste Anzeichen für eine koordinierte oder ungewöhnlich schnelle Verbreitung bestehen. Relevante Indikatoren sind ein sprunghafter Anstieg von Erwähnungen, gleichzeitige Postings verschiedener Accounts oder überdurchschnittliche Interaktionsraten in kurzer Zeit.

Medien- und Plattformresonanz: Wird der Vorfall ausschließlich auf einer Plattform diskutiert, oder gibt es Spillover zu weiteren digitalen oder medialen Öffentlichkeiten?

Während die erste Kategorie vor allem die Geschwindigkeit und Muster der Verbreitung bewertet, fragt diese Kategorie danach, welche Resonanzräume der Vorfall tatsächlich erreicht. Ein Inhalt verändert sein Risikoprofil erheblich, wenn er nicht nur innerhalb kleiner Nischen oder geschlossener Gruppen kursiert, sondern von größeren Accounts, relevanten Communities, journalistischen Medien, Branchenakteuren, Influencern oder politischen Akteuren aufgegriffen wird. Ebenso entscheidend ist die Plattformebene: Was zunächst nur in spezialisierten Foren oder Randplattformen sichtbar ist, kann eine ganz andere Wirkung entfalten, sobald es auf reichweitenstarken Kanälen wie LinkedIn, X oder TikTok auftaucht.

Ursprung und Glaubwürdigkeit der Absender: Wer verbreitet die Inhalte, und wie glaubwürdig sind diese Akteure?

Im Rahmen der Risikoabschätzung spielt nicht nur die Verbreitung eines Inhalts eine Rolle, sondern auch, wer ihn verbreitet. Die in Abschnitt 3.1 beschriebenen Prüffragen helfen hierbei als erste Orientierung. Für die Risikobewertung ist anschließend entscheidend, wie vertrauenswürdig und einflussreich die beteiligten Accounts sind. Inhalte, die lediglich von neu angelegten oder offensichtlich fragwürdigen Profilen aufgegriffen werden, sind in der Regel weniger kritisch einzuschätzen als solche, die durch bekannte Multiplikatoren, vernetzte Akteursgruppen, politische Profile oder glaubwürdig inszenierte Impersonationen verbreitet werden. Je stärker ein Inhalt von relevanten oder reichweitenstarken Absendern getragen wird, desto höher ist sein potenzielles Schad- und Reichweitenrisiko.

Potenzielles Schadenspotenzial: Welche realen, negativen Auswirkungen kann der Vorfall entfalten?

Anhand dieser Kategorie kann bewertet werden, welche konkreten Folgen aus dem Vorfall entstehen könnten. Dazu gehört, ob der Inhalt lediglich das allgemeine Meinungsbild beeinflusst, ob er reputationsschädigend wirkt – etwa gegenüber Führungspersonen der Organisation – oder ob er regulatorische Prozesse berührt. Ebenso fließt ein, ob operative Abläufe, Sicherheit oder sensible Daten betroffen sein könnten (z. B. im Kontext von Social Engineering oder Identitätsmissbrauch). Auch isolierte Fälschungen können hier eine hohe Risikostufe erreichen, wenn sie geeignet sind, Vertrauen zu beschädigen oder relevante Entscheidungen zu beeinflussen.

Dringlichkeit und zeitliche Dynamik: Wie schnell muss ein Verband oder Unternehmen reagieren, um Schaden zu vermeiden oder zu begrenzen?

Während Kategorie 1 die Ausbreitungsgeschwindigkeit eines Inhalts beschreibt, bewertet diese Kategorie die erforderliche Reaktionsgeschwindigkeit. Dringlichkeit entsteht etwa, wenn Stakeholder aktiv nachfragen, Medien Rückfragen stellen, Fehlinformationen operative Abläufe stören oder ein Zeitfenster droht, in dem Narrative „festfrieren“. Auch Fälle mit geringer Verbreitung können eine hohe Dringlichkeit aufweisen, wenn sie geschäftskritische Entscheidungen berühren oder ein regulatorisches Umfeld betreffen. Eine hohe Dringlichkeit weist darauf hin, dass unmittelbare Abstimmungen und vorbereitende Maßnahmen notwendig sind, um einen Reputations- oder Vertrauensschaden abzuwenden.

Die Gesamtpunktzahl, die sich aus diesem Scoring ableitet, dient als erste Orientierung dafür, welche weiteren Schritte folgen sollten. Diese sind in der Reaktionsmatrix je nach erreichtem Punktwert abgebildet.

Tabelle 2
Risikomatrix mit Handlungsanleitungen

Score	Risiko-Level	Handlung
5 - 10	Niedrig	Beobachtung, Monitoring verstärken, keine aktive Reaktion
11 - 15	Mittel	Gezielte Prüfung, Monitoring ausweiten, vorbereitende Kommunikationsschritte
16 - 20	Hoch	Interne Abstimmung, klare Kommunikationsstrategie vorbereiten, mögliche Interventionen bei weiterer Eskalation
21 - 25	Sehr hoch	Sofortige Reaktion, Aktivierung interner Prozesse, ggf. rechtliche Schritte und Krisenkommunikation

Die Risikomatrix kann je nach Verband oder Unternehmen angepasst und – sofern sinnvoll – auch in ein KI-gestütztes Bewertungssystem integriert werden. Voraussetzung ist jedoch, dass jede automatisierte Einschätzung vor operativen oder kommunikativen Entscheidungen durch menschliche Expertise überprüft wird. Entscheidend ist, die Matrix nicht als starres Schema, sondern als strukturierte Orientierungshilfe für eine konsistente und nachvollziehbare Bewertung zu verstehen.

Ergibt sich daraus die Notwendigkeit einer unmittelbaren Reaktion, folgt die Auswahl und Umsetzung geeigneter Reaktionsmethoden und -strategien, die im Folgenden dargestellt werden.

3.3 Wirksame Reaktionsmethoden und -strategien

Mindestens genauso wichtig wie die Identifikation und Analyse eines Desinformationsvorfalls ist die Frage, wie strukturell und kommunikativ darauf reagiert wird. Wirksame Reaktionen folgen **drei Grundprinzipien: Schnelligkeit**, um entstehende Informationslücken nicht unbesetzt zu lassen; **Klarheit**, um konsistente und belastbare Botschaften zu setzen; und **Anschlussfähigkeit**, damit Inhalte für die relevanten Zielgruppen verständlich und weitervermittelbar bleiben. Ebenso entscheidend ist eine **konsequente One-Voice-Policy**: Alle Beteiligten müssen in Tonalität, Inhalt und Zielsetzung abgestimmt kommunizieren, sonst verliert die Gegenreaktion an Glaubwürdigkeit.

Damit diese Grundprinzipien im Ernstfall greifen können, braucht es klar strukturierte Schritte, die sich am verfügbaren Zeitfenster, der gewählten Plattform und der kommunikativen Ausgangslage orientieren.

3.3.1 Zeitliche Maßnahmenkaskaden

Zeitfenster	Operative Schritte	Kommunikative Schritte	Framing und Narrativführung	Multiplikatoren und Ökosysteme
0–60 Minuten (Erstreaktion)	– Monitoring intensivieren (Keywords, Plattformen, Messenger-Hinweise) – Screenshots/ Links sichern – Plattform-Meldungen (Fake-Profil, Deepfake, Dokumente) – Interne Kurzabstimmung (Comms, PA, Recht, IT) – Erste Risikoeinordnung (Matrix)	– Nur dort reagieren, wo der Inhalt auftritt (kein Spillover) – Minimal-Statement falls nötig: „Uns liegen Hinweise vor, wir prüfen.“ oder „Vertrauen ist der zentrale Wert unserer Arbeit. Die in Umlauf befindliche Behauptung basiert auf einem manipulierten Dokument und ist falsch. Richtig ist: Wir arbeiten weiterhin nach den öffentlich bekannten Prozessen und werden über Veränderungen transparent informieren.“ – Keine Spekulation, keine Debatte befeuern	– Erstes „Frame-Setting“: Benennung von Taktiken („Fake-Profil“, „verfälschter Kontext“) – Orientierung statt Erklärung: „Was wissen wir / was wissen wir nicht?“	– Frühzeitige Info an vertrauenswürdige interne Multiplikatoren (Vorstand, Mitglieder, zentrale Stakeholder) – Keine breite Aktivierung (Gefahr Spillover)

1–6 Stunden (Stabilisierung und Kontextualisierung)	– Genaue Musteranalyse – Technische Maßnahmen: Sperranträge, Kopien löschen lassen, Kontakt zu Plattform-Support – Klärung juristischer Schritte	– Plattformspezifische Klarstellung (LinkedIn sachlich, X knapp, Meta moderierend, TikTok visuell, Messenger zielgerichtet) – FAQ vorbereiten – Interne Info: Lagebild und Empfehlung	– Kontexte anbieten („Warum diese Darstellung irreführend ist“) ohne das Narrativ zu wiederholen – Anschlussfähige Narrative setzen: Sicherheit, Verlässlichkeit, Orientierung	– Aktivierung glaubwürdiger Partner (z. B. Branchenverbände, Expert*innen, Mitglieder) – nicht automatisch öffentlich, ggf. nur zur Unterstützung der Einordnung
6–24 Stunden (Einordnung, Stabilisierung, Präzision)	– Vollständige Risikoanalyse abschließen und verbreiten – Langform-Klarstellung vorbereiten – Koordinierte Schutzmaßnahmen, ggf. mit Sicherheitsbehörden	– Konsistente Gegenrede mit maximaler Reichweite und Autorität – Proaktive Kommunikation über weitere Kanäle, wenn nötig (z. B. Medienanfragen)	– Stabilisierung des Rahmens: Glaubwürdigkeit, Transparenz, Sachlichkeit – Storytelling einsetzen: „Was wirklich passiert ist (Protagonist und struktureller Antagonist) – und wieso es relevant ist“	– Multiplikatoren breiter aktivieren, falls nötig (Expert*innen, Partnerorganisationen, externe Validierungen) – Framing in vertrauenswürdigen Ökosystemen verankern (Branchenmedien, Newsletter etc.)

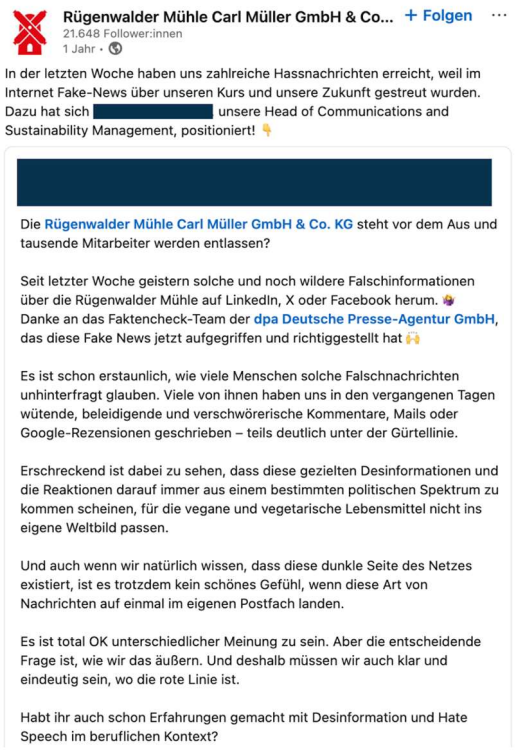
3.3.2 Plattform-spezifische Reaktionsschritte

Während die grundlegenden Kommunikationsprinzipien für alle Zeiträume und Fälle von Desinformation gelten, unterscheiden sich die konkreten Reaktionsschritte je nach Plattform deutlich. Eine wirksame Reaktion orientiert sich daher immer auch an der Logik des jeweiligen Kanals. Gleichzeitig gilt der Grundsatz, **Desinformation möglichst dort zu adressieren, wo sie entstanden ist, um keinen unnötigen Spillover in weitere Öffentlichkeiten auszulösen.** Im Folgenden werden die zentralen Plattformen skizziert, auf denen Verbände und Unternehmen am häufigsten mit Desinformation konfrontiert werden, und wie darauf reagiert werden sollte.

LinkedIn: Fachöffentlichkeit, Reputation und klare Einordnung

LinkedIn ist für Verbände und Unternehmen besonders relevant, weil hier professionelle Zielgruppen, Branchenkontakte, politische Akteure und Medienvertreter*innen aktiv sind. Inhalte verbreiten sich vergleichsweise langsam, wirken aber stark reputations- und meinungsbildend.

Abbildung 2
Beispiel einer Gegenrede auf LinkedIn



Bei Desinformationsfällen eignet sich LinkedIn für strukturierte Einordnungen, professionelle Klarstellungen und präzise Botschaften, die später als Referenzen dienen können. Wichtig ist, dass Klarstellungen sachlich, konsistent und überprüfbar sind, insbesondere bei Impersonation, manipulierten Medien oder verzerrten Behauptungen.

Der Fokus sollte darauf liegen, Transparenz herzustellen („Das wissen wir, das prüfen wir, das ist falsch“) und die Verbands- bzw. Unternehmensposition nachvollziehbar darzustellen. Da LinkedIn weniger anfällig für massive Bot- oder Troll-Operationen ist, eignet sich die Plattform häufig als erster Ansprechpunkt, insbesondere gegenüber Stakeholdern, Mitgliedern, Politik und Medien.

Meta-Plattformen (Instagram und Facebook): Reichweite, Communities und operatives Community-Management

Auf Instagram und Facebook können Falschinformationen schnell und teilweise innerhalb weniger Minuten große Reichweiten erzielen. Das Community-Management spielt hier eine zentrale Rolle: Kommentare müssen beobachtet, Fragen beantwortet und falsche Behauptungen eingeordnet werden.

Besonders wichtig ist die schnelle Moderation, das Melden von Fake-Profilen, die Eindämmung von Bot-Kommentaren und – wenn notwendig – eine gezielte Reichweitenbegrenzung (z. B. durch Einschränkung der Kommentarfunktion in absoluten Ausnahmefällen oder über Plattform-Supportkanäle).

Während Facebook stärker diskurs- und linkorientiert ist, sind Inhalte auf Instagram deutlich visueller, persönlicher und stärker durch kurze Videos, Story-Formate und Gesichter geprägt. Entsprechend wirken visuelle Klarstellungen, kurze Reels und personalisierte Statements auf Instagram oft besser als rein textliche Hinweise. Auf Facebook hingegen eignen sich strukturierte Posts, FAQ-Elemente oder erklärende Einordnungen.

Zentral bleibt: Orientierung klar, knapp und ohne Verstärkung manipulativer Inhalte geben. Bei Fake-Profilen, Deepfakes oder Fake-Dokumenten steht das technische Eingreifen im Vordergrund, inklusive melden, dokumentieren, löschen lassen und dabei immer ohne die Inhalte selbst erneut sichtbar zu machen.

X (ehemals Twitter) & Bluesky: Schnelligkeit, Dynamik und taktische Kurzformate

X ist weiterhin eine der dynamischsten Plattformen, jedoch seit dem Abbau von Moderations- und Sicherheitsstrukturen deutlich anfälliger für Desinformation, Bots und koordinierte Netzwerke. Organisationen sollten daher genau abwägen, ob und wie sie dort präsent bleiben.

Wenn eine Reaktion notwendig ist, gilt es kurz, präzise und eindeutig zu kommunizieren, sobald wesentliche Fakten gesichert sind. X eignet sich nicht für lange Erklärungen, sondern für klare Korrekturen, die als schnelle Referenzpunkte dienen („Fakt ist …“ / „Diese Behauptung ist frei erfunden, weil …“).

Abbildung 3
Beispiel einer Gegenrede auf X

Bluesky weist ähnliche Dynamiken auf, allerdings mit geringerer Politisierung und bisher niedrigerem Manipulationsrisiko. Reaktionen können hier vergleichbar kurz und klar erfolgen, mit etwas mehr Raum für Kontext, da Diskussionen strukturierter verlaufen.

Die zentrale Leitlogik lautet auf diesen vor allem Text-basierten Plattformen, dass man früh, sachlich und wiederholbar reagieren und gleichzeitig sorgfältig abwägen muss, ob eine Intervention die Verbreitung nicht unbeabsichtigt verstärkt. Inhalte, die bislang nur sehr begrenzt oder nur in sehr radikalisierten Milieus sichtbar sind, sollten nicht durch übermäßige Reaktion in zusätzliche Öffentlichkeiten getragen werden.

TikTok: Visuelle Klarstellungen und zugängliche Kontexte

TikTok folgt einer eigenen Dynamik, weil Inhalte hier vor allem über visuelle und emotionale Eindrücke wirken und sich sehr stark entlang algorithmischer Trends verbreiten. Auch beiläufig produzierte Videos können schnell große Reichweiten erzielen, besonders dann, wenn sie emotional aufgeladen sind oder auf visuellen Manipulationen beruhen.

Komplexere Themen benötigen eine reduzierte, aber nicht vereinfachende Einordnung. Ziel ist es, Orientierung zu geben, ohne in Alarmismus, Polemik oder unbeabsichtigte Sichtbarkeitssteigerung zu verfallen. TikTok ist besonders relevant bei Deepfakes oder visuell manipulierten Inhalten, da diese hier besonders schnell viral gehen.

Für Verbände und Unternehmen bedeutet das, dass Klarstellungen nicht primär textlich, sondern über kurze, visuell verständliche Formate erfolgen sollten, die die Kernbotschaft innerhalb weniger Sekunden erfassbar machen. Besonders wirkungsvoll sind Reaktionen, die einen kursierenden Inhalt direkt aufgreifen – etwa über Stitch- oder Duett-Formate. Dabei sollte jedoch niemals der manipulierte Teil des ursprünglichen Videos erneut gezeigt werden, sondern ausschließlich der Kontext, der erforderlich ist, um die Falschinformation einzuordnen und zu korrigieren.

Messenger-Dienste (WhatsApp, Signal, Telegram): Geschlossene Dynamiken und zielgerichtete Korrektur

Messenger-Dienste unterscheiden sich grundlegend von öffentlichen Plattformen, da sich Inhalte dort in geschlossenen Gruppen, vertrauensbasiert, fragmentiert und für Organisationen oft zunächst unsichtbar verbreiten. Hinweise aus der Belegschaft, aus Mitgliedsorganisationen oder aus Communitys sind deshalb besonders wichtig, weil sie häufig frühzeitig auf problematische Inhalte hinweisen („Das kursiert gerade in meiner Gruppe“).

Da Kommunikation in Messengern sehr direkt und persönlich erfolgt, sollten Klarstellungen – sofern angemessen und möglich – gezielt an die relevanten Gruppen oder Multiplikatoren adressiert werden. Weil hier in der Regel sehr spezifische Zielgruppen angesprochen werden, können Falschinformationen in der Klarstellung auch ausdrücklich benannt und inhaltlich korrigiert werden, ohne dass dies zu einer breiten zusätzlichen Sichtbarkeit führt. Entsprechend wichtig ist die sorgfältige Dokumentation eingehender Hinweise (Screenshots, Zeitpunkte, Gruppenkontexte), um Monitoring und Risikoabschätzung zu unterstützen.

Bei gefährlichen Inhalten wie etwa Deepfakes, Fake-Dokumenten oder Social-Engineering-Versuchen, sollten technische oder juristische Schritte frühzeitig geprüft und eingeleitet werden, da Messengerdienste häufig Ausgangspunkte für koordinierte Angriffe oder Identitätsmissbrauch sind.

3.3.3 Reaktionslogik

Anhand der bisherigen Faktoren lässt sich ableiten, in welchen Zeithorizonten welche Maßnahmen sinnvoll sind, wie die Plattformauswahl getroffen werden sollte und welche kommunikativen Spezifika zu berücksichtigen sind. So lässt sich nun präzisieren, welche Mittel der strategischen Kommunikation eingesetzt werden können, um Desinformationsnarrative wirksam zu entkräften.

Die folgenden Schritte greifen insbesondere dann, wenn die Risikomatrix (siehe Abschnitt 3.2) einen Score im oberen Bereich (zum Beispiel 21 bis 25 Punkte) ergibt und damit die Entscheidung getroffen wurde, dass eine unmittelbare kommunikative Reaktion erforderlich ist. Einzelne Elemente können jedoch auch bei mittlerem Risiko in abgeschwächter Form genutzt werden. Nach jedem Schritt sollte kurz geprüft werden, ob sich die Lage beruhigt oder weiter zuspitzt. Wenn sich wenig Dynamik zeigt, genügt häufig die Rückkehr in

den Monitoring-Modus; wenn der Vorfall an Fahrt gewinnt, ist der nächste Schritt angezeigt.

1. Schritt: Vor die Welle kommen (Prebunking, sofern möglich)

Prebunking bezeichnet das frühzeitige Einordnen oder Vorwegnehmen eines erwartbaren falschen Narrativs, bevor es sich verbreitet. Ziel ist es, das eigene Umfeld vorbeugend zu informieren und damit weniger anfällig für spätere Manipulationsversuche zu machen.

Entscheidungslogik:

Dieser Schritt ist nur möglich, wenn bereits vor dem eigentlichen Auftreten klar ist, welches Narrativ voraussichtlich verbreitet wird, etwa im Umfeld bekannter Akteure, erwartbarer Kampagnen oder sensibler regulatorischer Entscheidungen.

Mustertext (präventive Orientierung):

„In den kommenden Tagen kann es zu irreführenden Behauptungen rund um [Thema] kommen. Solche Darstellungen folgen erfahrungsgemäß bekannten Mustern, die darauf abzielen, Verunsicherung zu erzeugen. Wir möchten daher frühzeitig einordnen, worum es in der Sache tatsächlich geht, welche Methoden zur Verbreitung solcher Inhalte erfahrungsgemäß genutzt werden und wie wir von unserer Seite in den nächsten Schritten vorgehen werden."

---

2. Schritt: Radikale Transparenz herstellen

Tritt ein verdächtiges Element von Desinformation auf, so ist es unabdingbar möglichst früh zu benennen, was bekannt ist, was unklar ist und wie weiter vorgegangen wird. Gerade in den ersten Stunden reduziert eine nüchterne, transparente Einordnung Unsicherheit und verhindert, dass ein Informationsvakuum entsteht, das von Desinformation gefüllt wird.

Entscheidungslogik:

Wenn die Faktenlage noch nicht vollständig geklärt ist, wird zunächst nur der Prozess kommuniziert: "Wir haben den Vorfall erkannt, wir prüfen, wir melden uns wieder." Sobald zentrale Fakten verlässlich vorliegen, kann in den nächsten Schritt übergegangen werden.

Mustertext (kurzes öffentliches Erststatement):

„Uns liegen seit [Zeitpunkt] Hinweise auf irreführende Inhalte zu [Thema] vor. Wir nehmen diese Hinweise ernst und prüfen aktuell, wie es zu diesen Darstellungen gekommen ist. Unter folgender Seite finden Sie die geprüften Informationen zu dem Sachverhalt in der aktuellen Fassung: [Link]. Sobald belastbare Informationen vorliegen, werden wir diese transparent teilen und unsere nächsten Schritte erläutern."

3. Schritt: Taktiken sichtbar machen

Sobald klar ist, dass es sich um Desinformation oder eine andere Art der Manipulation handelt, kann die zugrunde liegende Methode benannt werden, zum Beispiel Impersonation, verzerrte Behauptungen, manipulierte Medien oder gefälschte Dokumente. Dadurch wird das Muster erkennbar und verliert an Glaubwürdigkeit.

Entscheidungslogik:

Dieser Schritt sollte erst erfolgen, wenn sichergestellt ist, dass es sich tatsächlich um eine Fälschung oder gezielte Manipulation handelt. Wo noch Zweifel bestehen, bleibt es bei Transparenz über den Prüfprozess. Wenn die Taktik eindeutig identifiziert ist, kann sie benannt und eingeordnet werden.

Mustertext (öffentliche Einordnung der Methode):

„Die aktuell kursierende Darstellung beruht auf einem gefälschten Dokument, das nicht von [Name] stammt. Layout und Absenderangaben weichen von unseren offiziellen Mitteilungen ab, wie sich hier eigenständig überprüfen lässt [Link]. Es handelt sich um einen Manipulationsversuch, den wir bereits bei den zuständigen Stellen und der Plattform gemeldet haben."

4. Schritt: Kontextualisierte Botschaften statt reiner Fakten

Wenn es explizit darum geht, eine Falschinformation zu entkräften, hat sich eine Struktur bewährt, die grob dem Prinzip „richtig – falsch – richtig" folgt: zuerst die eigene Kernbotschaft, dann die Einordnung der Falschbehauptung, anschließend erneut der eigene Rahmen.

Eine wirksame Reaktion stellt jedoch immer auch einen Bezug zur erlebbaren Realität her. Muss man eine Falschinformation gegenüber einer Zielgruppe adressieren, die beispielsweise ein hohes Sicherheitsbedürfnis hat, dann sollte durch ein klares und abgrenzendes Framing sichtbar werden, warum die manipulativen Akteure gegen Sicherheit arbeiten, während die eigene Organisation Sicherheit verkörpert.

Ergänzend können Storytelling-Elemente eingesetzt werden, etwa indem deutlich gemacht wird, wer die betroffene Organisation ist (Protagonist), welches strukturelle Problem oder welche verzerrte Darstellung gegenübersteht (Antagonist), und welches Zielbild verfolgt wird. So entsteht eine nachvollziehbare Erzählung, die Orientierung gibt, ohne die ursprüngliche Desinformation zu reproduzieren.

Entscheidungslogik:

Dieser Schritt eignet sich besonders, wenn zentrale Tatsachen nachweislich falsch sind und der betroffene Verband oder das betroffene Unternehmen über belastbare Gegeninformationen verfügen. Ziel ist nicht, jede einzelne Behauptung zu zerpflücken, sondern den Kern der Sache verständlich zu machen und das eigene Narrativ zu stabilisieren.

Mustertext (Struktur „richtig – falsch – richtig“):

„Richtig ist: [Name] arbeitet täglich daran, Verlässlichkeit und Sicherheit für [Mitglieder/Kunden/Partner] zu gewährleisten. Unsere Prozesse folgen klar definierten Standards, die regelmäßig durch unabhängige Stellen überprüft werden.

Falsch ist: Die aktuell verbreitete Darstellung verzerrt diese Realität. Sie basiert auf einem [manipulierten Video/gefälschten Dokument/einer erfundenen Behauptung], das den Eindruck erwecken soll, wir würden gegen zentrale Sicherheits- oder Qualitätsprinzipien verstoßen. Das Gegenteil ist der Fall. Die Quelle der Darstellung verfolgt erkennbar das Ziel, Vertrauen zu untergraben und Unsicherheit zu erzeugen.

Richtig bleibt: Unser Auftrag ist stabil: Wir schützen [Interessen/Zielgruppen/Themen] durch transparente Verfahren, klare Verantwortlichkeiten und überprüfbare Standards. Deshalb stellen wir alle relevanten Informationen offen bereit und aktualisieren diese fortlaufend. Wer Orientierung sucht, findet bei uns verlässliche Fakten – nicht manipulative Zuspitzungen.“

---

5. Schritt: Emotionen adressieren

Faktenkorrekturen allein reichen in vielen Fällen nicht aus. Wer verunsichert ist, braucht neben Informationen auch das Gefühl, dass seine Sorge gesehen wird. Ziel ist es, Unsicherheit zu adressieren, ohne zu dramatisieren oder Spekulationen zu bedienen. Dabei bietet es sich an, möglichst hohe Identifikation zu schaffen, etwa durch Einbezug von Führungspersonal oder von Personen aus der Belegschaft, die für die Zielgruppen glaubwürdig sind. Narrative Brücken können helfen, indem an bekannte Emotionen oder Erfahrungen angeknüpft und die Richtung behutsam neu gesetzt wird.

Entscheidungslogik:

Dieser Schritt ist vor allem dann wichtig, wenn Rückmeldungen von Mitgliedern, Mitarbeitenden, Kunden oder Medien zeigen, dass der Vorfall Irritation oder Vertrauensverlust

auslöst. Wenn die Resonanz niedrig bleibt und kaum Rückfragen kommen, kann er abgeschwächter erfolgen.

Mustertext (Adressierung von Verunsicherung):

„Wir wissen, dass die kursierenden Behauptungen verunsichern können. Vertrauen in [Branche/Organisation] ist für viele ein wichtiger Anker. Gerade deshalb ist es uns wichtig, die Situation transparent zu erklären und deutlich zu machen, was an den Darstellungen falsch ist und wie wir tatsächlich vorgehen."

---

6. Schritt: Reaktionen in glaubwürdige Ökosysteme einbetten

Botschaften wirken stärker, wenn sie nicht alleinstehen, sondern von vertrauenswürdigen Akteuren und Institutionen gestützt werden. Dazu gehören zum Beispiel Branchenverbände, unabhängige Expert*innen, Aufsichtsbehörden oder langjährige Partner. Diese müssen so niedrigschwellig wie möglich befähigt werden, authentisch die Falschinformationen zu entkräften (siehe Kapitel 5).

Entscheidungslogik:

Wenn absehbar ist, dass der Vorfall über die eigene Kommunikationsreichweite hinaus Auswirkungen haben kann, sollte geprüft werden, welche Partner für die Einordnung geeignet sind. In manchen Fällen genügt ein stilles Briefing, in anderen ist eine gemeinsame oder flankierende Stellungnahme sinnvoll.

Mustertext (Ansprache an Partner, nicht öffentlich):

„Aktuell kursieren irreführende Darstellungen zu [Thema], die auch für die Wahrnehmung unserer Branche relevant sein können. Wir haben die wesentlichen Punkte geprüft und eine kurze Einordnung vorbereitet. Wir freuen uns, wenn Sie diese in Ihren Gesprächen oder Formaten berücksichtigen. Uns ist wichtig, dass ein realistisches Bild der Lage erhalten bleibt."

---

7. Schritt: Melden, löschen, begrenzen

Bei klaren Verstößen wie Fake-Profilen, Deepfakes, rassistischen, sexistischen oder antisemitischen Inhalten, gefälschten Dokumenten, Bot-Netzwerken oder rechtlichen Risiken sind technische und rechtliche Schritte zentral: melden, verbergen, entfernen lassen, Reichweite begrenzen. Dieser Schritt läuft meist parallel zur Kommunikation.

Entscheidungslogik:

Immer dann, wenn ein Inhalt gegen Plattformregeln oder geltendes Recht verstößt oder eindeutig auf Identitätsmissbrauch beruht, sollten Meldungen an Plattformen,

gegebenenfalls an Behörden sowie an interne Sicherheitsstellen erfolgen. Nach Umsetzung der Maßnahmen sollte geprüft werden, ob die Kommunikationsaktivitäten angepasst werden können, weil die Sichtbarkeit der Inhalte sinkt.

Mustertext (Hinweis in einer Klarstellung):

„Wir haben die verfälschten Inhalte bei der Plattform zur Löschung gemeldet und die zuständigen Stellen über den Vorfall informiert. Sollten Ihnen ähnliche Inhalte begegnen, freuen wir uns über Hinweise an [Kontaktadresse], damit wir schnell reagieren können."

---

8. Kommunikation der langen Linien

Wenn die akute Phase eingeordnet ist, geht es darum, die eigenen Grundlinien zu stabilisieren und über einen längeren Zeitraum sichtbar zu halten. Dazu gehört, die gleiche Botschaft langfristig konsistent zu wiederholen, gegnerische Narrative in geeigneten Formaten einzuordnen und zu entkräften, Hintergrundseiten auf der Website zu aktualisieren sowie Hinweise in Newslettern oder Beiträgen für Mitglieder und Stakeholder zu verankern.

Entscheidungslogik:

Dieser Schritt ist besonders wichtig, wenn der Vorfall Themen berührt, die langfristig reputationsrelevant sind, etwa Vertrauen in Produkte, Geschäftsmodelle oder regulatorische Prozesse. Wenn sich zeigt, dass das Thema den Verband oder das Unternehmen länger begleiten wird, sollte aus der Einzelfallkommunikation eine dauerhafte, inhaltlich konsistente Linie werden.

Mustertext (langfristige Einordnung, zum Beispiel Website oder Newsletter):

„Sicherheit ist die zentrale Voraussetzung für das Funktionieren unserer Branche. Die Ereignisse der vergangenen Tage haben gezeigt, wie schnell irreführende Informationen die Wahrnehmung von [Thema/Branche] beeinflussen können. Deshalb bündeln wir auf dieser Seite die wichtigsten Fakten, Hintergründe und Ansprechpersonen. Unser Ziel ist, nachvollziehbar zu machen, wie wir arbeiten, welche Standards gelten und wie wir mit Hinweisen auf mögliche Desinformation umgehen."

Diese acht Schritte bieten einen Rahmen, an dem sich Kommunikationsverantwortliche der bayerischen Wirtschaft in hochdynamischen Situationen orientieren können.

3.4 Nachbereitung und *Lessons Learned*

Wenn die akute Phase nach einem Desinformationsvorfall abgeschlossen ist, beginnt die Nachbereitungsphase, die häufig unterschätzt wird, aber entscheidend dafür ist, wie widerstandsfähig ein Verband oder Unternehmen langfristig wird. Zwei Aspekte stehen im Mittelpunkt:

– die präzise Dokumentation des Geschehenen, sowohl für rechtliche Fragestellungen als auch zur späteren Klassifizierung des eigenen Risikoprofils, und
– das Ableiten von Optimierungspotenzialen für zukünftige Fälle („Lessons Learned“).

Damit die Nachbereitung wirksam ist, sollte sie in ein strukturiertes Abschlussdokument münden, das sowohl Erkenntnisse als auch konkrete Folgeaktionen, Verantwortlichkeiten und Zeitpläne enthält. Die folgenden Elemente bilden den Standardaufbau.

Prozessqualität: Haben unsere internen Abläufe getragen?

Zu Beginn der Nachbereitung steht die Frage, ob die internen Strukturen im Ernstfall funktioniert haben. Entscheidend ist nicht, ob ein Vorfall besonders komplex oder herausfordernd war, sondern ob die Abläufe verlässlich gegriffen haben.

Dazu gehört die Prüfung,

– wie schnell Warnsignale erkannt und weitergeleitet wurden,
– ob Rollen und Freigaben klar waren und ob die Abstimmung zwischen Kommunikation, Public Affairs, IT, Recht und Führung reibungslos funktioniert hat.

Auch Verzögerungen, Reibungspunkte oder fehlende Ressourcen werden an dieser Stelle sichtbar. Ziel dieses Schritts ist eine nüchterne Bewertung der „Maschinerie“: Wo lief der Prozess stabil, und wo braucht es Anpassungen, damit zukünftige Fälle schneller oder sauberer bearbeitet werden können?

Kommunikationswirkung: Haben unsere Botschaften erreicht, was sie sollten?

Anschließend wird die Wirkung der eigenen Kommunikation bewertet. Dabei geht es darum, ob die Botschaften tatsächlich Orientierung gegen Desinformation geschaffen haben. Relevant ist,

– wie Stakeholder, Mitglieder oder Kunden reagiert haben,
– welche Rückfragen eingingen
– und ob die gewählte Tonalität Vertrauen gestärkt oder Unsicherheit erzeugt hat.

Ebenso wichtig ist der Blick auf die Verbreitungsdynamik:

– Wurden Klarstellungen häufiger geteilt als die Falschbehauptung, oder blieb das Gegennarrativ dominierend?
– Wurden die Grundprinzipien – Schnelligkeit, Klarheit, Anschlussfähigkeit und One-Voice-Policy – sichtbar eingehalten?

So kann beurteilt werden, ob die gewählten Botschaften wirksam waren und wo die kommunikative Linie künftig angepasst werden sollte.

Dynamikbegrenzung: Wurde die Verbreitung erfolgreich eingeordnet oder gestoppt?

Die zentrale Wirksamkeitsfrage jeder abschließenden Analyse von Maßnahmen gegen Desinformation ist: **Hat sie die Dynamik gebremst oder nicht?** Daher wird in diesem Abschnitt geprüft,

- ob sich die Reichweite der Falschinformation nach der Klarstellung verringert hat,
- ob Plattformmaßnahmen wie Meldungen oder Löschungen tatsächlich durchgeführt wurden,
- und ob sich der Vorfall stabilisieren ließ, sodass wieder in den Monitoring-Modus übergegangen werden konnte.

Ebenso relevant ist,

- ob zusätzliche Eskalationsschritte notwendig waren oder ob die Reaktion früh genug gegriffen hat, um das Narrativ einzuordnen.

Anhand dieser Fragestellungen und Bewertungskriterien soll eine Einschätzung darüber getroffen werden, ob die Organisation nicht nur reagiert, sondern die Dynamik tatsächlich kontrolliert hat.

Vertrauensebene: Wie hat der Vorfall die Beziehung zu zentralen Gruppen beeinflusst?

Über den kurzfristigen Verlauf hinaus entscheidet vor allem die Vertrauensebene darüber, wie gut ein Verband oder ein Unternehmen aus einem Desinformationsvorfall hervorgeht. Deshalb wird geprüft,

- ob sich das Vertrauen relevanter Gruppen – etwa Medien, Mitglieder, politische Akteure oder Branchenpartner – verändert hat.

Sichtbar wird dies beispielsweise durch die Tonalität von Rückmeldungen, die Verlässlichkeit in der Zusammenarbeit oder die Frage, ob Verunsicherung nach der Einordnung spürbar abgenommen hat. Dies ist wichtig, um zu verstehen, ob nicht nur der Vorfall behoben wurde, sondern ob auch die langfristige Glaubwürdigkeit stabil geblieben ist.

Ableitung eines strukturierten Maßnahmenpakets

Die Erkenntnisse aus den Analyseperspektiven werden abschließend in ein integriertes Maßnahmenpaket überführt, in dem die zuvor identifizierten Schwachstellen adressiert werden sollen. Alle Maßnahmen werden schließlich mit klaren Verantwortlichkeiten, realistischen Zeitrahmen und einem Prioritätsgrad versehen, sodass ein verbindlicher Handlungsplan entsteht. Wo möglich, sollte dieses Wissen verbands- oder unternehmensweit zugänglich gemacht werden, um einen einheitlichen Wissensstand zu gewährleisten und Silodenken im Verband oder Unternehmen zu vermeiden.

4 Erweiterte Leitlinien

Handlungsorientierung für dynamische Krisensituationen

4.1 Don’ts – Verhaltensweisen, die das Problem verstärken

Viele gut gemeinte Reaktionen können die Lage verschlimmern, indem sie die manipulative Erzählung erst sichtbar machen, emotional eskalieren oder unbeabsichtigt die Glaubwürdigkeit der Angreifer stärken. Deshalb gilt es, folgende Muster konsequent zu vermeiden:

Manipulative Narrative wiederholen:

Auch zur Widerlegung sollten manipulative Behauptungen nicht Wort für Wort wiedergegeben werden. Jede Wiederholung – selbst im Rahmen einer Korrektur – erhöht die Sichtbarkeit und Verankerung der Falschinformation.

Warum vermeiden?

Wiederholte Aussagen erscheinen Menschen schneller vertraut und damit glaubwürdiger. Plattform-Algorithmen verstärken außerdem Inhalte, die häufig genannt werden, unabhängig davon, ob zustimmend oder widersprechend.

Mit Fakten isoliert kontern:

Kurze, rein faktische Gegendarstellungen („Das ist falsch.“) reichen selten aus. Sie liefern keine Orientierung und erreichen insbesondere verunsicherte Zielgruppen nicht.

Warum vermeiden?

Fakten ohne Kontext wirken kalt und wenig anschlussfähig. Menschen folgen eher Erzählmustern, Bedeutungen und emotionaler Einordnung als reinen Datenpunkten. Dadurch bleibt die Falschinformation oft wirkmächtiger als die Korrektur.

Zynismus, Abwertung oder Herablassung:

Spöttische oder herablassende Reaktionen beschädigen die eigene Glaubwürdigkeit, selbst wenn die Gegenseite offensichtlich manipulativ agiert.

Warum vermeiden?

Zynismus verstärkt Polarisierung, provoziert Gegenangriffe und lässt unbeteiligte Beobachter zweifeln, ob der Verband oder das Unternehmen souverän handelt. In sensiblen oder politisierten Themenfeldern wirken solche Reaktionen schnell unsachlich oder unsicher.

Lange Freigabeschleifen in Akutsituationen:

Wenn die Abstimmung über ein kurzes Erststatement länger als 3–6 Stunden dauert, entsteht ein Informationsvakuum, das von Dritten gefüllt wird.

Warum vermeiden?

Schweigen oder Verzögerung wirken wie Intransparenz oder fehlende Kontrolle. Dadurch können sich manipulative Inhalte früh festsetzen und weitere Dynamiken entwickeln.

Widersprüchlich auftreten:

Uneinheitliche Aussagen, wechselnde Formulierungen oder voneinander abweichende Sprecher*innen untergraben die Glaubwürdigkeit, auch dann, wenn die Fakten korrekt sind.

Warum vermeiden?

Inkonsistenz wird von Außenstehenden schnell als Unstimmigkeit und „Vertuschung“ interpretiert. Sie bietet zusätzliche Angriffsfläche für neue Falschbehauptungen.

4.2 Do’s – Kommunikationsverhalten mit hoher Wirksamkeit

Wirksame Gegenreaktionen auf Desinformation beruhen nicht allein auf der schnellen Bereitstellung korrekter Fakten. Entscheidend ist vielmehr, wie diese kommuniziert werden, in welchem Rahmen sie eingebettet sind und welche Anschlussfähigkeit sie für unterschiedliche Zielgruppen erzeugen. Die folgenden Do’s bilden den Kern eines wirkungsvollen kommunikativen Umgangs mit Desinformationsvorfällen und ergänzen die zuvor beschriebenen Prozess- und Plattformlogiken.

Schnell, transparent und einheitlich reagieren:

Zeit ist einer der entscheidenden Faktoren in Desinformationsdynamiken. Je früher ein Verband oder Unternehmen sichtbar Orientierung bietet, desto kleiner bleibt der Raum, in dem sich manipulative Inhalte festsetzen können. Bei der Gegenrede zählt dabei nicht nur die Qualität der Botschaft, sondern auch ihre Kontinuität und Wiedererkennbarkeit. Deshalb sollte vorbereiteter Content so gestaltet sein, dass er von Multiplikatoren unkompliziert in digitale wie analoge Räume weitergegeben werden kann – etwa in Branchen-Newsletter, interne Verteiler, Messenger-Gruppen oder Social-Media-Posts.

Warum wichtig?

Wiederholte Aussagen erscheinen Menschen schneller vertraut und damit glaubwürdiger. Plattform-Algorithmen verstärken zudem Inhalte, die häufig genannt werden, unabhängig davon, ob zustimmend oder widersprechend.

Orientierung statt Komplexität geben:

In der Akutphase zählt nicht immer Vollständigkeit, sondern vor allem auch Verlässlichkeit. Eine verständliche Einordnung („Was wissen wir? Was prüfen wir? Was stimmt nicht?“) wirkt stärker als komplexe Detailantworten.

Warum wichtig?

Verunsicherte Zielgruppen benötigen vor allem Klarheit und Struktur. Orientierung reduziert kognitive Belastung und erhöht die Wahrscheinlichkeit, dass Inhalte angenommen werden.

Eigenen Rahmen setzen – nicht in fremden Frames argumentieren:

Wirksam ist eine Kommunikation, die erklärt, was stimmt und wofür der Verband oder das Unternehmen steht, statt sich ausschließlich an gegnerischen Behauptungen abzuarbeiten. Der eigene Rahmen (z. B. in der Struktur „richtig – falsch – richtig“) verhindert, dass die Organisation in eine defensive Rolle rutscht oder sich unbeabsichtigt am Gegennarrativ entlanghangelt.

Warum wichtig?

Eigene Rahmen verhindern, dass gegnerische Narrative dominieren. Sie geben Zielgruppen Stabilität und erleichtern es, die gewünschte Perspektive einzunehmen, statt sich an der manipulativen Erzählung zu orientieren.

Klare, faktenbasierte und respektvolle Tonalität wahren:

Auch unter Druck sollte Kommunikation ruhig, sachlich und respektvoll bleiben. Abwertungen, Zynismus oder Eskalationsrhetorik schwächen die Glaubwürdigkeit und bieten Angriffsfläche für weitere manipulative Deutungen. Eine ruhige Sprache, gestützt auf verständliche Zahlen, Daten und Fakten, hilft dabei, Vertrauen zu halten – selbst in hoch polarisierten Situationen. Dafür sollten wesentliche Fakten, Links, Prozesse, Prüfschritte und interne Expertise jederzeit schnell verfügbar sein. Das ermöglicht zügige Reaktionen, vermeidet Fehler unter Zeitdruck und erhöht die Nachvollziehbarkeit der eigenen Position.

Warum wichtig?

Emotional eskalierende Sprache verstärkt Lagerdenken und wirkt auf unbeteiligte Beobachter*innen schnell unsouverän. Eine respektvolle, faktenbasierte Tonalität signalisiert Kontrolle, Professionalität und Verlässlichkeit. Gleichzeitig steigt die Wahrscheinlichkeit, dass Zielgruppen Klarstellungen akzeptieren und weitertragen, weil sie überprüfbar und konsistent sind.

Digitale Ansprechbarkeit klar signalisieren:

Sichtbare und verlässliche Kommunikationskanäle verhindern, dass Stakeholder in Unsicherheit geraten oder mangels Orientierung auf alternative, weniger vertrauenswürdige Informationsquellen ausweichen. Dazu gehören eindeutig benannte Anlaufstellen, ein nachvollziehbarer Veröffentlichungsrhythmus sowie transparente Hinweise darauf, wann nächste Informationen zu erwarten sind.

Warum wichtig?

Ansprechbarkeit wirkt vertrauensbildend und erleichtert es Zielgruppen, Rückfragen zu stellen, bevor sie auf Desinformation reagieren oder diese weiterverbreiten.

5 Maßnahmen zur langfristigen Prävention und Vorbereitung

Strukturelle, technische und kommunikative Grundlagen für nachhaltige Resilienz

5.1 Organisatorische Vorbereitung: Strukturen, Rollen und Entscheidungsfähigkeit

Wie bereits vielfach deutlich wurde, entstehen Geschwindigkeit und Klarheit im Umgang mit Desinformation nicht spontan, sondern sind das Ergebnis vorheriger Strukturentscheidungen. Verbände und Unternehmen, die im Ernstfall erst Zuständigkeiten klären müssen oder im Modus der Alltagskommunikation verharren, verlieren wertvolle Zeit. Klare Rollen, Verantwortlichkeiten und Entscheidungswege für den Ernstfall sind daher die Grundlage jeder wirksamen Prävention.

Bewährt hat sich in diesem Kontext ein Krisenstabsmodell, das kurzfristig aktiviert und ebenso klar wieder deaktiviert werden kann. Dieser Krisenstab sollte aus einer kleinen, entscheidungsfähigen Gruppe bestehen, deren Rollen vorab eindeutig definiert sind. Aus jeder der folgenden Funktionen sollte eine Person – maximal zwei – benannt werden, mit klarer Aufgabenverteilung:

- Kommunikation / Pressestelle:
  Nimmt Hinweise entgegen, führt eine erste inhaltliche Einordnung durch und gibt eine kommunikative Empfehlung ab. Bei Freigabe koordiniert sie die operative Umsetzung, erstellt Klarstellungen und steuert die Medienarbeit.

- Public Affairs / politische Kommunikation:
  Bindet relevante politische oder institutionelle Stakeholder ein, sorgt für die gezielte Distribution der Gegenrede und koordiniert externe Kontakte, etwa zu Plattformen, Behörden oder Verbänden. Zudem bewertet sie Kommunikationsmaßnahmen aus politischer und regulatorischer Perspektive mit.

- Leitungsebene mit Entscheidungsbefugnis:
  Trifft zeitnah verbindliche Entscheidungen und erteilt finale Freigaben, insbesondere bei Eskalationen, rechtlichen Risiken oder hoher öffentlicher Aufmerksamkeit.

- Optional – IT-Sicherheit und Recht (je nach Falltyp):
  Unterstützen bei technischen Gegenmaßnahmen, der Durchsetzung von Meldungen gegenüber Plattformen oder Sicherheitsbehörden sowie bei der Prüfung und Einleitung rechtlicher Schritte gegen Angreifer.

Der Krisenstab muss befugt sein, kurzfristige Entscheidungen zu treffen, Prioritäten zu setzen und Freigaben zu erteilen, und das auch außerhalb regulärer Arbeitszeiten. Im akuten Fall sollte er mindestens morgens und abends für jeweils etwa 30 Minuten tagen. Ergänzend ist klar zu regeln, unter welchen Bedingungen der Krisenstab aktiviert wird und wann der Übergang zurück in den Normalbetrieb erfolgt.

5.2 Krisenszenarien: Vorbereitung durch antizipiertes Handeln

Neben klaren Strukturen und Zuständigkeiten ist die Antizipation und Simulation möglicher Desinformationsangriffe ein zentraler Bestandteil langfristiger Prävention. Krisenszenarien sollten sich dabei an realistischen Falltypen orientieren, wie sie in den vorangegangenen Kapiteln beschrieben wurden. Ziel ist es, potenzielle Desinformationsnarrative, typische Absender, charakteristische Angriffsmuster – etwa die Kombination aus verzerrten Narrativen, Deepfakes und Bot-Kampagnen – sowie mögliche Eskalationsdynamiken systematisch zu erfassen und entlang einer Phasenlogik einmal vollständig durchzuspielen.

Angesichts der hohen Dynamik aktueller Desinformationsentwicklungen empfiehlt sich hierfür ein regelmäßiger Übungsrhythmus, idealerweise mindestens einmal jährlich. In Form von Simulationen oder Planspielen kann der Krisenstab unter realistischen Zeitbedingungen trainieren, wie Hinweise eingehen, wie sie bewertet werden, welche Entscheidungen erforderlich sind und wie kommunikative Reaktionen ausgestaltet werden. In diesen Übungen wird bereits vor dem Ernstfall sichtbar, wo Prozesse greifen, wo Unklarheiten bestehen und an welchen Stellen wertvolle Zeit verloren geht.

Auf Basis dieser Szenarien sollten zudem Narrative, Kernbotschaften und Narrative entwickelt werden, die den zuvor beschriebenen Prinzipien folgen. Diese Inhalte dienen ausdrücklich nicht als starre Textbausteine, sondern als inhaltliche Orientierung, die im Ernstfall angepasst werden kann, ohne bei null beginnen zu müssen.

5.3 Narrativ-Allianzen aufbauen

Wenn es darum geht, mit der eigenen Botschaft durchzudringen, haben faktenbasierte Akteure einen strukturellen Nachteil gegenüber destruktiven Akteuren: Sie können weder beliebig viele widersprüchliche Botschaften parallel spielen noch künstliche Verstärkung einsetzen. Wie in Abschnitt 3.3 und den erweiterten Leitlinien deutlich wurde, lässt sich dieser Nachteil nur teilweise ausgleichen, wenn im Ernstfall auf ein belastbares Netzwerk an Multiplikatoren zurückgegriffen werden kann, die die Gegenrede schnell und glaubwürdig mittragen.

Die vier Kommunikationswissenschaftler*innen Michael Etter, Patrick Haack, Simone Mariconda und Marta Pizzetti beschreiben diesen Umstand wie folgt:

"To effectively combat disinformation, organizations must spread the perception that fake news lacks widespread credibility **not only because it is demonstrably false but also because others don't believe it.** That means crafting a multichannel strategy that addresses the falsehoods while also signaling that experts, peers, and other key stakeholders recognize the disinformation. **The goal isn't just to correct the record; it's to show that the company's reputation remains intact in the eyes of those who matter.**"[12]

Solche Allianzen entstehen jedoch nicht spontan, sondern müssen langfristig aufgebaut und gepflegt werden. Dazu gehört zunächst die gezielte Identifikation relevanter Multiplikatoren nach Glaubwürdigkeit, Nähe zu relevanten Zielgruppen und tatsächlichem Einflusspotenzial. Je nach Kontext können dies Fachpersonen, Branchenakteure, Journalist*innen, Influencer oder auch eigene Mitarbeitende sein.

Entscheidend ist, diese Akteure nicht als bloße Verteiler zu behandeln, sondern als belastbare Partner. Im Vorfeld braucht es daher eine verlässliche Kommunikationsinfrastruktur, beispielsweise in Form eines gemeinsamen Workspaces mit Untergruppen, regelmäßiger Einordnung sensibler Themen und einem gemeinsamen Verständnis darüber, welche Standards gelten. Im konkreten Vorfall geht es dann nicht um eine breite Alarmierung, sondern um eine gezielte Aktivierung mit klaren, weiterleitbaren Informationen, etwa über kurze Talking Points, ein kompaktes FAQ und ein knappes Lagebild. Diese Inhalte müssen jederzeit maximal niedrigschwellig, verständlich und schnell verfügbar sein, damit die Hemmschwelle für potenzielle Partner gering bleibt und sie eigenständig zur Entkräftung von Desinformation beitragen können.

[12] Etter, M. et al. (2025): *How to counter fake news*. Harvard Business Review. https://hbr.org/2025/09/how-to-counter-fake-news

6 Ausblick

Entscheidend ist organisatorische Lernfähigkeit

Dieser Leitfaden folgt dem Anspruch, für Verbände und Unternehmen nicht nur die Herausforderungen und Dynamiken von Desinformation verständlich aufzubereiten, sondern auch den aktuellen Stand wirksamer Gegenmaßnahmen praxisnah darzustellen. Wie bereits mehrfach deutlich wurde, handelt es sich bei Desinformation im wirtschaftlichen Kontext jedoch um ein Phänomen, das sich äußerst dynamisch entwickelt und in immer neuen Ausprägungen auftritt.

Daher steht abschließend über allem die fortwährende Empfehlung, auf Basis eigener Erfahrungswerte, aber auch anhand der Erfahrungen anderer wirtschaftlicher Akteure, aktueller Forschungsergebnisse sowie Ansätzen aus dem politischen Kontext, Kompetenzen regelmäßig weiterzuentwickeln, Maßnahmen anzupassen und das Bewusstsein innerhalb der eigenen Organisation kontinuierlich zu schärfen. Insbesondere für Verbände und Unternehmen liegt ein zentraler strategischer Vorteil darin, dass bereits zahlreiche potenzielle Multiplikatoren vorhanden sind, die – wenn sie richtig eingebunden werden – sowohl bei der frühzeitigen Identifikation als auch bei der Gegenrede einen erheblichen Mehrwert leisten können.

Es ist davon auszugehen, dass das Phänomen Desinformation in den kommenden Jahren weiter an Bedeutung gewinnen wird und Verbände wie auch Unternehmen zunehmend direkter, personalisierter und skalierter adressiert werden. Mit dem Übergang zu agentischen KI-Systemen ist dabei zu erwarten, dass Desinformationskampagnen nicht nur Inhalte automatisiert erzeugen, sondern eigenständig verbreiten, testen und strategisch anpassen können, etwa durch das parallele Ausspielen unterschiedlicher Narrative, die fortlaufend optimiert werden.

Vor diesem Hintergrund wird eine informationskompetente bayerische Wirtschaft, die auch außerhalb akuter Krisen ihre Kommunikation konsistent, authentisch und entlang klarer „langer Linien“ ausrichtet, zum entscheidenden Stabilitätsfaktor. Wer kontinuierlich Narrative anpasst, Beziehungen pflegt und Maßnahmen testet, bleibt dabei resilient gegen Desinformation.

7 Weitere Materialien

7.1 Weiterführende Literatur

Einordnung Desinformation im Verbands- und Unternehmenskontext

Berger, C. / Unzicker, K. (2024): *Große Mehrheit erkennt in Desinformation eine Gefahr für Demokratie und Zusammenhalt*. Bertelsmann Stiftung.
www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2024/februar/grosse-mehrheit-erkennt-in-desinformation-eine-gefahr-fuer-demokratie-und-zusammenhalt

University of Baltimore / CHEQ. (2019): *The Economic Cost of Fake News*. University of Baltimore / CHEQ.
s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf

Weltwirtschaftsforum. (2024): *Global Risks Report 2024 – Presseinformation (DE)*. Weltwirtschaftsforum.
www3.weforum.org/docs/WEF_GRR24_Press%20release_DE.pdf

Weltwirtschaftsforum. (2025): *Global Risks Report 2025: Conflict, environment and disinformation top threats*. Weltwirtschaftsforum.
www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/

Maßnahmen gegen Desinformation

Bateman, J. / Jackson, D. (2024): *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace.
carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide

Bitkom. (2024): *Maßnahmen gegen Desinformation und Deepfakes*. Bitkom.
www.bitkom.org/sites/main/files/2024-09/bitkom-policy-brief-massnahmen-gegen-desinformation-deepfakes.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2025): *Deepfakes – Risiken für Unternehmen*. BSI.
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Bundesverband Digitale Wirtschaft. (2024): *Whitepaper – Deepfakes – Eine Einordnung*. BVDW.
www.bvdw.org/news-und-publikationen/vertrauensverlust-in-digitale-medien-bvdw-whitepaper-nimmt-deepfakes-ins-visier/

CDR-Initiative. (2023): *Desinformation und Hate Speech – White Paper*. CDR-Initiative.
cdr-initiative.de/uploads/files/CDR_Initiative_WP_Desinformation_Hate_Speech.pdf

DISARM Foundation. (2025): *DISARM Framework*. DISARM Foundation. www.disarm.foundation/framework

Etter, M. et al. (2025): *How to counter fake news*. Harvard Business Review. hbr.org/2025/09/how-to-counter-fake-news

House of Lords Communications and Digital Committee. (2024): *The Future of News*. UK Parliament. publications.parliament.uk/pa/ld5901/ldselect/ldcomm/39/39.pdf

IDCARE. (2025): *What to do when your business is impersonated*. IDCARE Learning Centre. www.idcare.org/learning-centre/fact-sheets/what-to-do-when-your-business-is-impersonated

International Center for Journalists. (2025): *Disarming Disinformation: Brazil Case Study*. ICFJ. www.icfj.org/sites/default/files/2025-03/ICFJ%20Disarming%20Disinformation%20Brazil%20Case%20Study.pdf

Siebert, L. (2025): *Warum und wie Unternehmen und Verbände Ziel von Desinformation werden*. FORTITUDE. fortitudeinfo.substack.com/p/warum-und-wie-unternehmen-und-verbande

Schnoeller, J. (2021): *Public Arena Playbook*. Murmann Verlag. www.murmann-verlag.de/products/juri-schnoeller-public-arena-playbook

Republic of Latvia. (2025): *Handbook Against Disinformation*. State Chancellery of Latvia. www.mk.gov.lv/en/Handbook-Against-Disinformation

Wolff, U. (2024): *Desinformationsangriffe auf Unternehmen abwehren*. Springer Gabler. link.springer.com/book/10.1007/978-3-658-43755-8

Fallbeispiele

Alethea. (2023): *When crisis strikes, disinformation thrives*. Alethea. alethea.com/insights/when-crisis-strikes-disinformation-thrives

Auswärtiges Amt. (2024): *Technischer Bericht zur Desinformationskampagne „Doppelgänger“*. Auswärtiges Amt. www.auswaertiges-amt.de/resource/blob/2660362/73bcc0184167b438173e554ba2be2636/technischer-bericht-des-informationskampagne-doppelgaenger-data.pdf

Center for the Study of Democracy. (2025): *The Kremlin Playbook Against Offshore Wind Energy in Bulgaria*. CSD. csd.eu/publications/publication/the-kremlin-playbook-against-offshore-wind-energy-in-bulgaria/

Dunkel, M. (2025): *KI-Betrug: Bayer-Chef Bill Anderson wurde Deepfake-Opfer*. Capital. www.capital.de/wirtschaft-politik/ki-betrug--bayer-chef-bill-anderson-wurde-deepfake-opfer-35486154.html

Echtermann, A. (2022): *Fake-Kampagne: Werke von BASF, Siemens oder VW werden nicht wegen Energiekrise geschlossen*. Correctiv. correctiv.org/faktencheck/2022/12/08/fake-kampagne-werke-von-basf-siemens-oder-vw-werden-nicht-wegen-energiekrise-geschlossen/

Fenimore Harper Communications. (2025): *Can AI Cause a Bank Run?*. Fenimore Harper Communications. www.fenimoreharper.com/research/bankrun

Krause, M. (2025): *Börsengang? Bielefelder Unternehmen Dr. Oetker wehrt sich gegen Fake-News*. Neue Westfälische. www.nw.de/lokal/bielefeld/mitte/24107755_Boersengang-Bielefelder-Unternehmen-Dr.-Oetker-wehrt-sich-gegen-Fake-News-v1.html

Siebert, L. (2025): *Pharma und Gesundheit im Fadenkreuz von Desinformation*. FORTITUDE / Substack. fortitudeinfo.substack.com/p/pharma-und-gesundheit-im-fadenkreuz

Spiegel Online. (2022): *Aktienkurs von Insulinhersteller fällt nach Fake-Tweet*. Spiegel Online. www.spiegel.de/wirtschaft/unternehmen/twitter-chaos-aktienkurs-von-insulinhersteller-faellt-nach-fake-tweet-a-cd2eebad-54aa-4c33-81d9-6b37c78dd733

Tagesspiegel. (2025): *LLM-Grooming-Methode: Russland manipuliert offenbar westliche Chatbots für seine Propaganda*. Der Tagesspiegel. www.tagesspiegel.de/internationales/llm-grooming-methode-russland-manipuliert-offenbar-westliche-chatbots-fur-seine-propaganda-13370401.html

Vereinigung der Bayerischen Wirtschaft e. V. (vbw). (2025): *Warnhinweis zu Fake-Profilen im Umlauf*. vbw auf Instagram. www.instagram.com/p/DM94t9gNOTD/

Wheaton, S. (2024): *When civil society resorts to fake news*. Politico Europe. www.politico.eu/newsletter/politico-eu-influence/when-civil-society-resorts-to-fake-news-2/

7.2 Mustertexte der Reaktionslogik

Schritt	Mustertext
Vor die Welle kommen (Prebunking, sofern möglich)	Präventive Orientierung: „In den kommenden Tagen kann es zu irreführenden Behauptungen rund um [Thema] kommen. Solche Darstellungen folgen erfahrungsgemäß bekannten Mustern, die darauf abzielen, Verunsicherung zu erzeugen. Wir möchten daher frühzeitig einordnen, worum es in der Sache tatsächlich geht, welche Methoden zur Verbreitung solcher Inhalte erfahrungsgemäß genutzt werden und wie wir von unserer Seite in den nächsten Schritten vorgehen werden.“
Radikale Transparenz herstellen	Kurzes öffentliches Erststatement: „Uns liegen seit [Zeitpunkt] Hinweise auf irreführende Inhalte zu [Thema] vor. Wir nehmen diese Hinweise ernst und prüfen aktuell, wie es zu diesen Darstellungen gekommen ist. Unter folgender Seite finden Sie die geprüften Informationen zu dem Sachverhalt in der aktuellen Fassung: [Link]. Sobald belastbare Informationen vorliegen, werden wir diese transparent teilen und unsere nächsten Schritte erläutern.“
Taktiken sichtbar machen	Öffentliche Einordnung der Methode: „Die aktuell kursierende Darstellung beruht auf einem gefälschten Dokument, das nicht von der [Name] stammt. Layout und Absenderangaben weichen von unseren offiziellen Mitteilungen ab, wie sich hier eigenständig überprüfen lässt [Link]. Es handelt sich um einen Manipulationsversuch, den wir bereits bei den zuständigen Stellen und der Plattform gemeldet haben.“
Kontextualisierte Botschaften statt reiner Fakten	Struktur „richtig – falsch – richtig“: „Richtig ist: Die [Name] arbeitet täglich daran, Verlässlichkeit und Sicherheit für [Mitglieder/Kunden/Partner] zu gewährleisten. Unsere Prozesse folgen klar definierten Standards, die regelmäßig durch unabhängige Stellen überprüft werden. Falsch ist: Die aktuell verbreitete Darstellung verzerrt diese Realität. Sie basiert auf einem [manipulierten Video/gefälschten Dokument/einer erfundenen Behauptung], das den Eindruck erwecken soll, wir würden gegen zentrale Sicherheits- oder Qualitätsprinzipien verstoßen. Das Gegenteil ist der Fall. Die Quelle der Darstellung verfolgt erkennbar das Ziel, Vertrauen zu untergraben und Unsicherheit zu erzeugen.

	Richtig bleibt: Unser Auftrag ist stabil: Wir schützen [Interessen/Zielgruppen/Themen] durch transparente Verfahren, klare Verantwortlichkeiten und überprüfbare Standards. Deshalb stellen wir alle relevanten Informationen offen bereit und aktualisieren diese fortlaufend. Wer Orientierung sucht, findet bei uns verlässliche Fakten – nicht manipulative Zuspitzungen.“
Emotionen adressieren	Adressierung von Verunsicherung: „Wir wissen, dass die kursierenden Behauptungen verunsichern können. Vertrauen in [Branche/Organisation] ist für viele ein wichtiger Anker. Gerade deshalb ist es uns wichtig, die Situation transparent zu erklären und deutlich zu machen, was an den Darstellungen falsch ist und wie wir tatsächlich vorgehen.“
Reaktionen in glaubwürdige Ökosysteme einbetten	Ansprache an Partner, nicht öffentlich: „Aktuell kursieren irreführende Darstellungen zu [Thema], die auch für die Wahrnehmung unserer Branche relevant sein können. Wir haben die wesentlichen Punkte geprüft und eine kurze Einordnung vorbereitet. Wir freuen uns, wenn Sie diese in Ihren Gesprächen oder Formaten berücksichtigen. Uns ist wichtig, dass ein realistisches Bild der Lage erhalten bleibt.“
Melden, löschen, begrenzen	Hinweis in einer Klarstellung: „Wir haben die verfälschten Inhalte bei der Plattform zur Löschung gemeldet und die zuständigen Stellen über den Vorfall informiert. Sollten Ihnen ähnliche Inhalte begegnen, freuen wir uns über Hinweise an [Kontaktadresse], damit wir schnell reagieren können.“
Kommunikation der langen Linien	Langfristige Einordnung, zum Beispiel Website oder Newsletter: „Sicherheit ist die zentrale Voraussetzung für das Funktionieren unserer Branche. Die Ereignisse der vergangenen Tage haben gezeigt, wie schnell irreführende Informationen die Wahrnehmung von [Thema/Branche] beeinflussen können. Deshalb bündeln wir auf dieser Seite die wichtigsten Fakten, Hintergründe und Ansprechpersonen. Unser Ziel ist, nachvollziehbar zu machen, wie wir arbeiten, welche Standards gelten und wie wir mit Hinweisen auf mögliche Desinformation umgehen.“

Ansprechpartner/Impressum

Stefanie Zormaier
Geschäftsführerin Abteilung Operations, Marketing, IKT

Telefon 089-551 78-274
stefanie.zormaier@vbw-bayern.de

Melanie Tropp
Abteilung Operations, Marketing, IKT

Telefon 089-551 78-187
melanie.tropp@vbw-bayern.de

Impressum
Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

Weiterer Beteiligter

Linus Siebert
FORTITUDE

Telefon 0176 2380 7138
linus@fortitude-info.com