



Fake oder Fakt

Wie Unternehmen Desinformation
begegnen und ihre Reputation
schützen können

Einleitung	05
Begriff und Funktionsweise von Desinformation	06
Begriffsbestimmung	06
Arten von Desinformation	07
Funktionsweise und Verbreitung von Desinformation	09
Aktualität des Themas	10
Relevanz für Unternehmen (Branchenperspektive)	11
Strategien gegen Desinformationskampagnen	12
Fazit und Ausblick	15
Ansprechpartner:innen	16

Einleitung

In der heutigen Zeit ist Desinformation nicht mehr nur ein Randphänomen des digitalen Raums. Es ist vielmehr ein systemisches gesellschaftliches Problem, welches uns im Internet zunehmend begegnet. Die Verbreitung unzutreffender oder irreführender Inhalte gefährdet das Wohlergehen von Menschen und die Stabilität der Gesellschaft. Auch wenn solche Inhalte nicht zwangsläufig gegen Gesetze verstoßen, können sie gesellschaftliche Spaltung verstärken, die Umsetzung politischer Vorhaben beeinträchtigen und dem Vertrauen in demokratische Institutionen schaden.

Ein öffentlicher Vertrauensverlust kann enorme Auswirkungen haben. Dahinter verbergen sich Risiken für Demokratie und Freiheit und somit auch für unsere Gesellschaft als Ganzes.

Aus dieser gesellschaftlichen Ausgangslage ergibt sich unmittelbar die Relevanz für Unternehmen. Denn Firmen und ihre Produkte werden im Markt nicht allein über objektive Fakten bewertet, sondern über Wahrnehmungen, die sich in digitalen Kanälen rasch bilden, verstärken und verfestigen. In einem Umfeld algorithmischer Verstärkung und hoher Reichweitendynamik, können manipulative Narrative die Reputation von Unternehmen und damit auch die Grundlage für Kundennachfrage, Kooperationsfähigkeit und Investorenvertrauen angreifen. Für Organisationen ist Desinformation deshalb ein Risiko mit

direktem Einfluss auf Top und Bottom Line. Auf der Top Line können falsche oder manipulierte Behauptungen bspw. über Produktsicherheit oder Compliance als Folge Kaufentscheidungen, Vertragsabschlüsse und Partnerschaften negativ beeinträchtigen. Auf der Bottom Line entstehen Kosten durch Krisenkommunikation, forensische Prüfung, Rechtsdurchsetzung, Monitoring, interne Eskalation sowie erhöhten Support-Aufwand.

Kurzum lässt sich sagen: Wo Vertrauen fällt, steigen Kosten und zwar messbar. Unternehmen sollten Desinformation daher als strategisches Risiko behandeln, das Reputation, Marktverhalten und Wertschöpfung gleichzeitig betrifft. Desinformation gehört daher raus aus der reaktiven „PR-Feuerwehr“ hinein in eine aktive, unternehmensweite Steuerung.

Ein öffentlicher Vertrauensverlust kann erhebliche negative Auswirkungen haben.

Begriff und Funktionsweise von Desinformation

Begriffsbestimmung

„Desinformation“ bezeichnet die absichtliche Verbreitung falscher, ungenauer oder irreführender Informationen. Ziel ist es, die Wahrnehmung von Menschen bewusst zu täuschen, zu manipulieren oder Akteuren damit Schaden zuzufügen.¹ Davon zu unterscheiden ist der Begriff „Misinformation“. Dieser beschreibt die unbeabsichtigte Verbreitung falscher Inhalte ohne Täuschungsabsicht. Mögliche Gründe hierfür sind bspw. unzureichende Recherche, fehlerhafte Interpretation von Fakten oder Missverständnisse. Der zentrale Unterschied zwischen Fehl- und Desinformation ist die Absicht: Desinformation will täuschen, Misinformation nicht (s. Abb. 1).²

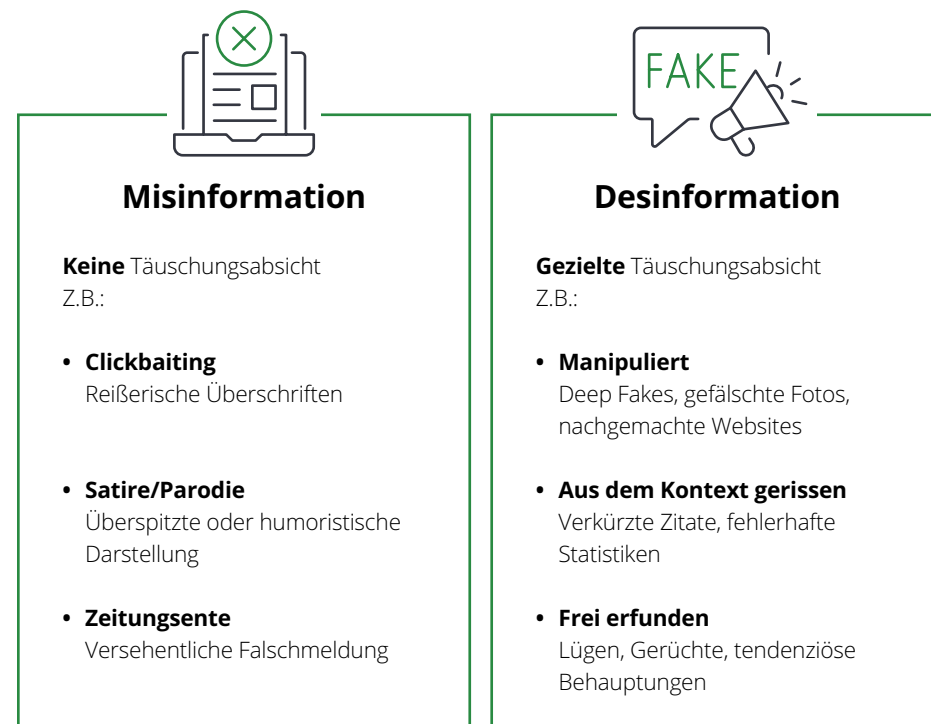
Theoretische Ansätze charakterisieren Desinformation wie folgt:

- Inhalte sind nachweislich falsch oder täuschend
- Mögliche Verursachung von gesellschaftlichen Schäden,
- Gezielte Koordination von bestimmten Akteuren
- Dient politischen oder wirtschaftlichen Zielen

Inhaltlich beziehen sich Desinformationskampagnen oftmals auf Themen wie Politik, Wahlen, Gesundheit oder Wirtschaft.

Desinformation wird häufig als Teil von systematisch gesteuerten Kampagnen verbreitet. Verschiedene Akteure nutzen sie in unterschiedlichen Formaten, z.B. als Text, Bild oder Video. Ziel ist es, bestehende Konflikte zu verschärfen, Wut und starke Gefühle anzuheizen, den gesellschaftlichen Zusammenhalt und das Vertrauen in demokratische und rechtsstaatliche Institutionen zu schwächen. Besonders ausländische Staaten setzen Desinformation gezielt als Werkzeug zur Einflussnahme ein.³

Abb. 1 – Beispiele von Mis- (Fehl-) und Desinformation



Quelle: Bundesregierung/BPA

Arten von Desinformation

Desinformationskampagnen setzen dabei auf folgende Manipulationswerkzeuge:



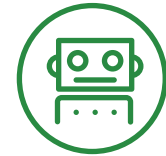
Fake News

Fake News sind falsche oder irreführende Inhalte, die mit Absicht verbreitet werden, um Personen, Institutionen oder Organisationen zu schädigen. Dafür werden Gerüchte und Falschmeldungen mit gefälschten „Beweisen“ versehen und zu einer scheinbar stimmigen Nachricht zusammengefügt. Häufig werden auch Bilder aus dem Kontext gerissen, um eine Geschichte gezielt zu verändern.



Deep Fakes

Deep Fakes sind benannt nach der Kombination von „Deep Learning“ und „Fake“ und stellen eine besondere Form von Fake News dar. Sie nutzen die starke Wirkung von Bild und Ton, um Menschen gezielt zu täuschen. Sie sind künstlich erstellte oder stark veränderte Videos, Bilder und Tonspuren. Sie entstehen mit künstlicher Intelligenz (KI) und wirken oft so echt, dass selbst Fachleute sie nur schwer von realen Aufnahmen unterscheiden können. Ihr Einsatz reicht von harmlosen Spaßclips bis hin zu gefährlicher politischer Propaganda. Damit haben Deep Fakes das Potenzial, das Vertrauen in Medieninhalte grundlegend zu erschüttern.⁴



Social Bots

Social Bots sind automatisierte Profile in sozialen Netzwerken. Sie geben sich als echte Menschen aus, oftmals mit Profilbild und erfundenem Namen. Ihr Ziel ist es, Gespräche und Meinungen zu beeinflussen, indem sie in großer Zahl Falschmeldungen teilen und weiterverbreiten. Solche Profile können automatisiert Beiträge mit bestimmten Schlagwörtern (Hashtags) in Umlauf bringen, anderen Profilen folgen, um deren Popularität größer erscheinen zu lassen, oder in großer Zahl Kommentare hinterlassen. Auf diese Weise stützen, verstärken oder widerlegen sie die darin geäußerten Meinungen.⁵



Trolle

Trolle sind Menschen, nicht Bots. Sie stören in sozialen Netzwerken absichtlich Gespräche, manipulieren Diskussionen und lenken sie vom Thema ab. Ihr Ziel ist die Provokation, Diffamierung und Polarisierung.



Sockenpuppen

Als Sockenpuppe gilt im Netzjargon ein Zweit- oder Mehrfachkonto, das von derselben Person betrieben wird. Solche Konten werden gezielt genutzt, um die öffentliche Meinung zu beeinflussen. Sie bestätigen sich in Diskussionen gegenseitig, sodass der Eindruck entsteht, mehrere unabhängige Personen tauschten sich aus. Dadurch werden Debatten unbemerkt beeinflusst. Eine Einzelposition wirkt wie eine verbreitete Mehrheitsmeinung.⁶

¹ Die Bundesregierung: „Was ist Desinformation?“ Bundesregierung, 12. Februar 2026.

² Bundesamt für Sicherheit in der Informationstechnik (BSI): „Desinformation im Internet.“ BSI, o.D.

³ Steffen, Nico; Kroon, Peter; Wiewiorra, Lukas: Verbreitung und Auswirkungen von Desinformation im Kontext des DSA & Online Plattformen. WIK Diskussionsbeitrag Nr. 546, Dezember 2025.

⁴ Landeszentrale für politische Bildung BadenWürttemberg (LpB BW): „Fake News.“ lpb-bw.de, o.D.

⁵ Bundesamt für Sicherheit in der Informationstechnik (BSI): „Exkurs: Social Bots und Chatbots.“ BSI, o.D.

⁶ Reuter, Markus: „FakeNews, Bots und Sockenpuppen – eine Begriffsklärung.“ netzpolitik.org, 29. November 2016.



Funktionsweise und Verbreitung von Desinformation

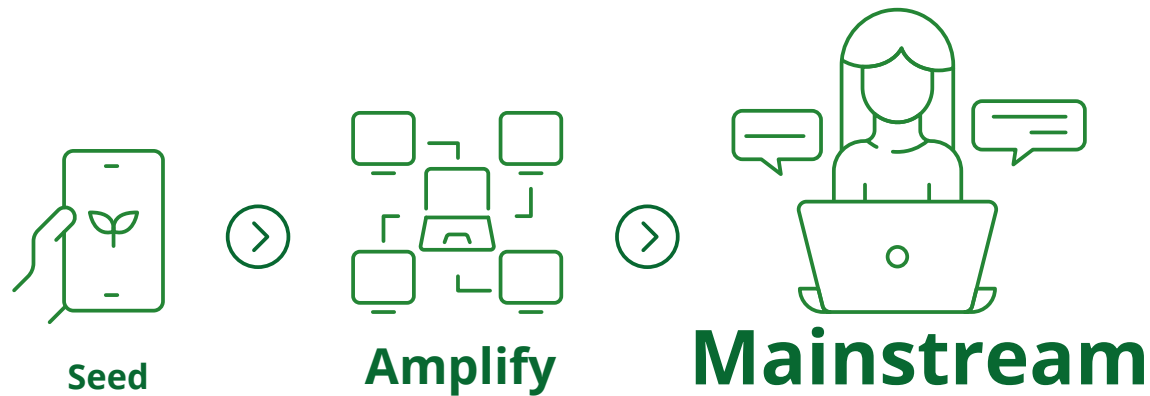
In sozialen Netzwerken kann sich Desinformation besonders rasch ausbreiten, weil ihre Funktionsweise auf dem Teilen und Weiterverbreiten von Inhalten beruht. Die Geschäftsmodelle von Plattformen sind darauf ausgerichtet, Verweildauer und Interaktionen zu steigern. Ihre Empfehlungsalgorithmen bevorzugen Inhalte, die voraussichtlich viele Klicks, Kommentare oder Shares erzeugen. Emotional aufgeladene und polarisierende Beiträge, einschließlich solcher mit Desinformation, fügen sich besonders gut in diese Logik ein. Dadurch kann es zu einer unbeabsichtigten, aber strukturell bedingten Bevorzugung solcher Inhalte kommen. Diese Funktionslogik und die eingesetzten Algorithmen auf Plattformen lassen sich gezielt missbrauchen, um Reichweite künstlich zu erhöhen und Glaubwürdigkeit vorzutäuschen.⁷

Die Funktionsweise moderner Desinformationskampagnen folgt typischerweise einem Lebenszyklus von Seed – Amplify – Mainstream. In der Seed-Phase wird zunächst die Desinformation in Nischenkanälen platziert. Anschließend erfolgt die Verbreitung in der Amplify-Phase über u.a. orchestrierte Bot-Netze, Sockenpuppen-Accounts und Influencer-Ökosysteme. In der Mainstream-Phase gelangen die Narrative in die breitere Öffentlichkeit. Dies geschieht dadurch, dass größere Accounts die Desinformation aufgreifen oder diese durch reaktive Stellungnahmen in die Massenmedien gelangt.⁸

Indikatoren für entstehende Kampagnen können anomale Wachstumsraten, ungewöhnliche Sprach-/Geografiemuster, dichte Re-Post-Cluster und hochgradig redundante Schlagwörter sein.

Abb. 2 – Lebenszyklus von Desinformationskampagnen

Systematische Desinformationskampagnen skalieren Reichweite in Wellen: von der Platzierung in Nischen über orchestrierte Verstärkung bis zur Übernahme in die breite Öffentlichkeit.



⁷ Steffen, Nico; Kroon, Peter; Wiewiorra, Lukas: Verbreitung und Auswirkungen von Desinformation im Kontext des DSA & Online Plattformen. WIK Diskussionsbeitrag Nr. 546, Dezember 2025.

⁸ Basel Institute on Governance: „How mushroom sites and disinformation stand in the way of combating corruption in Bulgaria.“ Basel Institute on Governance, 14. Oktober 2024.

Aktualität des Themas

Möglichkeiten zur Verfälschung medialer Darstellungen gibt es seit vielen Jahren. Besonders bei Fotos ist seit Langem bekannt, dass sie auf unterschiedliche Weise bearbeitet werden können. Deutlich schwieriger war es über lange Zeit, dynamische Inhalte wie Videos oder Audioaufnahmen in hoher Qualität und somit für die Öffentlichkeit glaubwürdig zu verändern. Durch Anwendung von generativer KI ist die Erstellung von täuschend echten Inhalten so einfach wie noch nie: Fälschungen können mit vergleichsweise geringem Aufwand und wenig Spezialwissen in

Sekundenschnelle erstellt werden. Dies verschärft die Bedrohungslage durch Desinformation. In Kombination mit der gezielten Manipulation der Empfehlungsalgorithmen von Plattformen stellt generative KI einen zentralen Treiber für die Verbreitung von Desinformationskampagnen dar.⁹



Relevanz für Unternehmen (Branchenperspektive)

In der Vergangenheit wurde Desinformation häufig eingesetzt, um demokratische Abläufe zu stören, Wahlen zu beeinflussen und das Vertrauen der Bevölkerung in staatliche Institutionen sowie den Journalismus zu schwächen. Inzwischen hat sich der Schwerpunkt verlagert: Akteure und kriminelle Gruppen nutzen dieselben Taktiken, Methoden und Verbreitungskanäle wie frühere politische Desinformationskampagnen, um Unternehmen anzugreifen und zu schädigen. Dies führt dazu, dass Desinformation eine zunehmende Bedrohung für Unternehmen darstellt.¹⁰ Laut dem Global Risks Report 2024 des Weltwirtschaftsforums (WEF) gehört Desinformation zu dem am höchsten eingeschätzten Risiko.¹¹ Damit wird Desinformation zunehmend zu einer unternehmensbezogenen Angriffsform. Diese adressiert nicht primär IT-Systeme, sondern die zentrale ökonomische Ressource: Vertrauen – und damit die Reputation von Unternehmen und Marken.

Warum ist Reputation dabei geschäftskritisch? Weil sie die Wahrnehmung von Unternehmen, Produkten und Managemententscheidungen prägt. Diese Wahrnehmung lässt sich in betriebswirtschaftlich messbare Effekte übersetzen. Auf der Nachfrageseite zeigt empirische Forschung, dass negative Informationen über die Unternehmensreputation Markenhaltung und Kaufabsicht signifikant verschlechtern können. Reputation wirkt damit unmittelbar auf Kundenentscheidungen und damit

auf die Top Line. Auf der Kapitalmarktseite ist Reputation ein wesentlicher Bestandteil immaterieller Werttreiber und kann, insbesondere in Krisen, mit der Entwicklung von Shareholder Value und Kursreaktionen zusammenhängen.¹²

Unternehmen sehen sich daher zunehmend mit einem neuen Multirisikoprofil konfrontiert. In diesem konvergieren u.a. die folgenden Risiken miteinander:

- **Vertrauensverlust:** Desinformation untergräbt das Vertrauen in Organisationen, etwa durch manipulierte Kundenbewertungen, erfundene Meldungen über Geschäftspraktiken oder fingierte Aussagen von Führungskräften. Einmal verlorenes Vertrauen ist nur schwer zurückzugewinnen und schwächt sowohl die Markentreue als auch die Beziehungen zu wichtigen Stakeholdern.
- **Reputationsschäden:** Gezielte Desinformationskampagnen können den Ruf eines Unternehmens schwer und langfristig beschädigen. Verbreitet sich Desinformation schneller, als eine Organisation angemessen reagieren kann, bleibt bei Öffentlichkeit und Investorenschaft häufig ein dauerhafter negativer Eindruck zurück.
- **Störung operativer Abläufe:** Desinformation über bspw. Datenschutzvorfälle oder Produktmängel können operative

Abläufe erheblich beeinträchtigen. Die Folgen reichen von unnötigen Rückrufaktionen über behördliche Prüfungen bis hin zu finanziellen Verlusten.

- **Rechtliche und regulatorische Risiken:** Wenn der Eindruck entsteht, dass ein Unternehmen unzureichend gegen Desinformation vorgeht, kann dies rechtliche und aufsichtsrechtliche Konsequenzen haben, insbesondere, wenn Verbrauchende oder Märkte betroffen sind. Zugleich wird die Einhaltung relevanter Vorgaben zu digitalen Inhalten und Desinformationen (bspw. DSA und AI Act) zunehmend komplex.¹³

¹⁰ Roy, Priyanka: „Desinformation und ihre Auswirkungen auf Unternehmen: Strategien und Lösungen.“ SecurityInsider, 30. Juni 2025.

¹¹ World Economic Forum: „Global Risks 2024: At a turning point.“ Global Risks Report 2024, 10. Januar 2024.

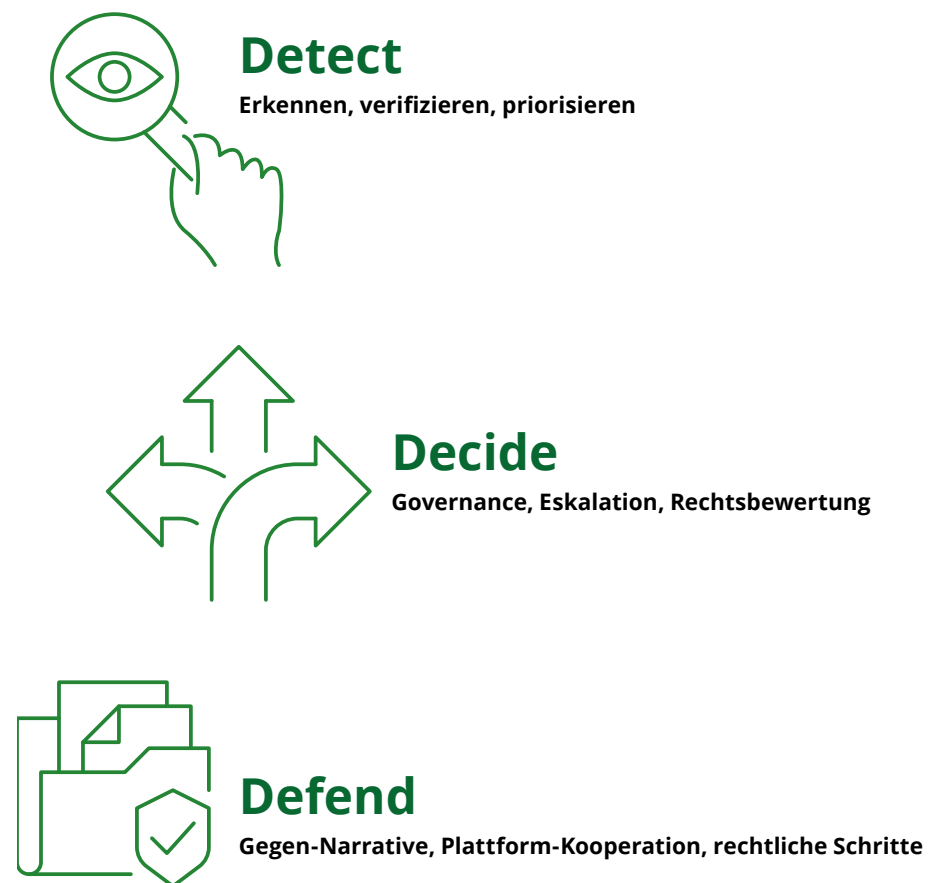
¹² Gatzert, Nadine: The Impact of Corporate Reputation and Reputation Damaging Events on Financial Performance: Empirical Evidence from the Literature. Working Paper, FAU, Version 4., September 2015.

¹³ Roy, Priyanka. „Desinformation und ihre Auswirkungen auf Unternehmen: Strategien und Lösungen.“ SecurityInsider, 30. Juni 2025.

Strategien gegen Desinformationskampagnen

Angesichts der zunehmenden Bedrohung durch Desinformation benötigen Organisationen eine vorausschauende, mehrstufige Strategie, um Integrität und öffentliches Vertrauen zu sichern. Dabei kann nach dem „Detect – Decide – Defend“-Framework vorgegangen werden. Desinformation berührt Governance-, Sicherheits- und Compliance-Domänen gleichermaßen. Daher ist es von zentralem Stellenwert, alle relevanten Stakeholder in diesen strategischen Prozess zu involvieren.

Abb. 3 – Ansatz zur strategischen Bekämpfung von Desinformation



Detect

Detect beschreibt ein belastbares Frühwarnsystem, das externe Signale durch Netzwerkanalysen ermittelt (z.B. in sozialen Netzwerken, Suchmaschinen, Foren) und interne Informationen (z.B. Kundenkontakte, Incident-Meldungen) integriert. Ziel ist es, aufkommende Narrative möglichst früh zu erkennen, technische Fälschungen zu verifizieren und Relevanz sowie Dringlichkeit zu bewerten. Damit können Folgeschritte faktenbasiert und verhältnismäßig definiert werden. Die Netzwerkanalyse beinhaltet eine kontinuierliche Beobachtung von Narrativen: Schlüsselwörter, Hashtags, Meme-Varianten und Bot-Accounts werden kontinuierlich analysiert und auf Anzeichen von Desinformation oder die Anbahnung einer koordinierten Desinformationskampagne analysiert.

Decide

Decide übersetzt die Erkenntnisse der vorangehenden Phase in klare, nachvollziehbare Entscheidungen. Es wird geregelt, wer wann mit welchem Mandat handelt, welche rechtlichen Optionen bestehen, wie mit Plattformen kooperiert wird und wann eine Kommunikation nach innen/außen erfolgt. Dies beinhaltet ein koordiniertes Incident-Management: Auf Basis des zugrunde liegenden Risikos werden geeignete Handlungsmaßnahmen ausgewählt. Diese könnten u.a. weiteres Monitoring, stille Takedown-Anträge und Plattform-Meldungen, proaktive Gegenkommunikation oder eine Kombination aus allem sein.

Defend

Defend bündelt kommunikative, organisatorische, technische und rechtliche Maßnahmen, um das Narrativ zu korrigieren, Schäden zu begrenzen, Vertrauen wiederherzustellen und künftige Angriffe zu erschweren. Dabei sind Plattform-Kooperation, Faktenchecks und die eigene Sensibilisierung die tragenden Säulen. Zentrale Aktivitäten im Rahmen der Defend-Phase können sein:

- **Gegenkommunikation nach dem „Truth Sandwich“-Prinzip:** klare Fakten, kurze Einordnung des Falschen, erneute Faktenfestigung, wo möglich mit visuellen Belegen (Dokumente, Bildmaterial mit Herkunftsnachweis).
- **Plattform-Kooperation:** priorisierte Meldungen über Trusted-Flagger-Kanäle, enge Abstimmung mit Fact-Checkern, direkte Ansprache von Plattformen zur Entfernung von falschen Inhalten.
- **Rechtliche Schritte:** Einleitung rechtlicher Maßnahmen gegen Fake-Domains, gezielte Takedowns sowie die Einleitung zivil-/strafrechtlicher Verfahren bei identifizierbaren und rückverfolgbaren Accounts.
- **Wiederherstellung und Stakeholder-Arbeit:** Neben der öffentlichen Korrektur sind interne und direkte Stakeholder-Informationen entscheidend. Mitarbeitende erhalten kommunikationsrelevante

Informationen, Kunden und Partner bekommen faktenbasierte Kurzbrieife, Investor-Relations adressiert potenzielle Marktmissverständnisse. In Fällen mit Kursrelevanz werden Markt-Trigger (z.B. Ad-hoc-Kommunikation) geprüft.

Eine Abwägung der zu treffenden Maßnahmen ist erforderlich. Nicht jede Falschmeldung verdient eine Bühne. Der Nutzen einer Korrektur muss deren Amplifikationsrisiko übersteigen. Juristische Maßnahmen können abschrecken, erzeugen aber gleichzeitig auch eine Sichtbarkeit. Zudem braucht es Konsistenz: Korrekturen sollten in denselben Kanälen/Sprachen erscheinen, in denen die Desinformation verbreitet wurde, und länger sichtbar bleiben als die ursprüngliche Meldung.



Fazit und Ausblick

Desinformation hat sich von einem Randthema zu einem strukturellen gesellschaftlichen sowie unternehmerischen Risiko entwickelt. Vor diesem Hintergrund ist Desinformation kein reines Kommunikationsproblem, sondern ein unternehmensweites Risiko: Sie greift Vertrauen an und wirkt damit direkt auf Reputation, Nachfrage und Kosten. Durch generative KI und plattformgetriebene Verstärkung steigen Geschwindigkeit und Reichweite koordinierter Kampagnen. Unternehmen verlieren dadurch Reaktionszeit. Ein wirksamer Schutz entsteht, wenn Organisationen Desinformation systematisch managen: früh erkennen (Detect), klar entscheiden (Decide) und konsequent reagieren (Defend) – abgestimmt über Kommunikation, Recht, Security, Risk und Compliance. Wer diese Routinen verankert, reduziert Schäden, stabilisiert Vertrauen und schützt die „Licence to operate“¹⁴ im digitalen öffentlichen Raum.

¹⁴ Begriffsdefinition: „Licence to operate“ = gesellschaftliche Akzeptanz eines Unternehmens und seines Geschäftsmodells.

Ansprechpartner:innen



Martin Ritter

Partner | Enterprise Risk
Tel: +49 151 58077794
maritter@deloitte.de



Maria Chernyshov

Senior Manager | Enterprise Risk
Tel: +49 151 12683741
machernyshov@deloitte.de

Literatur

Basel Institute on Governance. „How mushroom sites and disinformation stand in the way of combating corruption in Bulgaria.“ Basel Institute on Governance, 14. Oktober 2024. <https://baselgovernance.org/blog/how-mushroom-sites-and-disinformation-stand-way-combating-corruption-bulgaria> (Zugriff am 1.4.2026).

Bundesamt für Sicherheit in der Informationstechnik (BSI). „Desinformation im Internet.“ BSI, o.D. <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Desinformation/Desinformation.html> (Zugriff am 1.4.2026).

Bundesamt für Sicherheit in der Informationstechnik (BSI). „Exkurs: Social Bots und Chatbots.“ BSI, o.D. <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Exkurs-bots/social-bots.html> (Zugriff am 1.4.2026).

Die Bundesregierung. „Was ist Desinformation?“ Bundesregierung, 12. Februar 2026. <https://www.bundesregierung.de/breg-de/aktuelles/was-ist-desinformation-1875148> (Zugriff am 1.4.2026).

Gatzert, Nadine. The Impact of Corporate Reputation and Reputation Damaging Events on Financial Performance: Empirical Evidence from the Literature. Working Paper, Friedrich-Alexander-Universität Erlangen Nürnberg (FAU), Version 4., September 2015. https://www.vworm.rw.fau.de/files/2016/05/Reputation_Research_2015-09-04_WP.pdf (Zugriff am 1.4.2026).

Landeszentrale für politische Bildung Baden-Württemberg (LpB BW). „Fake News.“ lpb-bw.de, o.D. <https://www.lpb-bw.de/fake-news> (Zugriff am 1.4.2026).

Reuter, Markus. „Fake-News, Bots und Sockenpuppen – eine Begriffsklärung.“ netzpolitik.org, 29. November 2016. <https://netzpolitik.org/2016/fakenews-social-bots-sockenpuppen-begriffsklaerung/> (Zugriff am 1.4.2026).

Roy, Priyanka. „Desinformation und ihre Auswirkungen auf Unternehmen: Strategien und Lösungen.“ Security-Insider, 30. Juni 2025. <https://www.security-insider.de/desinformation-auswirkungen-unternehmen-strategien-loesungen-a-f9236be8ef60bb2ed0c2cc350c6f8c95/> (Zugriff am 1.4.2026).

Steffen, Nico; Kroon, Peter; Wiewiorra, Lukas. Verbreitung und Auswirkungen von Desinformation im Kontext des DSA & Online-Plattformen. WIK Diskussionsbeitrag Nr. 546, Dezember 2025. https://www.wik.org/fileadmin/user_upload/Unternehmen/Veroeffentlichungen/Diskus/2025/WIK_Diskussionsbeitrag_Nr_546.pdf (Zugriff am 1.4.2026).

World Economic Forum. „Global Risks 2024: At a turning point.“ Global Risks Report 2024, 10. Januar 2024. <https://www.weforum.org/publications/global-risks-report-2024/in-full/global-risks-2024-at-a-turning-point/> (Zugriff am 1.4.2026).



Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter www.deloitte.com/de/ueberUns.

Deloitte bietet führende Prüfungs- und Beratungsleistungen für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeitenden liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, und unsere Kunden bei Wandel und Wachstum unterstützen. Deloitte baut auf eine 180-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 470.000 Mitarbeitenden von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeitende oder Bevollmächtigte haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.

Stand 07/2026

