GEFAHREN UND HANDLUNGSBEDARFE IM KONTEXT DESINFORMATION, KI UND CYBERSICHERHEIT FÜR KMU

Herausforderungen und Bedrohungen für Unternehmen

Gezielte Falschinformationen stellen eine signifikante und zunehmende Gefahr für Unternehmen dar. Das World Economic Forum gibt in seinem Global Risks Report 2026 **Des- und Misinformation als zweitgrößtes kurzfristiges Risiko** an, nachdem es 2024 und 2025 bereits als größtes solches Risiko eingeschätzt wurde. Auch die langfristige Prognose erwartet das Themenfeld unter den Top 5 Risiken in den nächsten zehn Jahren. Insbesondere Gefahren durch KI werden im langfristigen Blick immer höher bewertet. Weltweit wurden die **Kosten durch Falschinformationen** bereits 2019 auf rund 80 Mrd. US-Dollar geschätzt, bei jährlich zunehmender Gefahr.

Sie können dabei unter anderem zu höherer Arbeitslosigkeit und geringerer Produktion führen, wie Analysen der Universität Bonn auf Basis von US-Daten zeigen. Ein plötzlicher Anstieg irreführender Informationen – sogenannte Fake-News-Schocks – wirkt demnach wie ein "aggregierter Unsicherheitsschock". Selbst wenn Marktakteure Falschmeldungen erkennen, wissen sie nicht, wie andere reagieren werden. Diese Unsicherheit hemmt Investitionen und wirtschaftliche Aktivität. Auch wird davor gewarnt, dass Falschmeldungen zu Produkten, Lieferketten oder Finanzen Entscheidungen von Investoren oder Kunden verzerren können. Fake-Accounts in den sozialen Medien können in wenigen Stunden virale Kampagnen gegen Unternehmen fabrizieren, die das Vertrauen der Kund:innen erodieren lassen.

Beispiele von Unternehmen als Ziel von digitaler Desinformation, Manipulationen und Shitstorms

***"Osterhase-Verbot"**: Lidl und Aldi geritten im Frühjahr 2025 in die Schusslinie rechter Shitstorms, da Nutzer:innen in sozialen Medien die Discounter für angebliche "Osterhasen-Verbote" verantwortlich machten, vor einer "Islamisierung Deutschlands" warnten und zu Boykotten aufriefen. Missachtet wurde hierbei, dass die Bezeichnung "Sitzhase" als branchenüblicher Produktcode zur Unterscheidung von Formen verwendet wird, während weiterhin auch Millionen traditionelle "Osterhasen" verkauft werden.*

***Deepfakes von Bayer-CEO Bill Anderson:** Ein Beispiel für die Gefahr von Deepfakes lieferte ein mit KI gefälschtes Video des Bayer-CEO Bill Anderson aus dem Februar 2025. Dieses zeigt ihn in einer australischen Fernsehsendung, wie er für ein neues Abnehmpräparat wirbt, was es in der Realität jedoch gar nicht gibt. Schaden und Motiv blieben unklar. Zuvor wurde Anderson bereits Opfer eines WhatsApp-Fakes, in dem er vermeintlich Bayer-Mitarbeitende um Hilfe bei einer "heiklen Angelegenheit" bittet. Ziel dieses Fakes war es vermutlich, durch Links Schad- oder Spionagesoftware in die Bayer-Systeme zu schleusen.*

***Rheinmetall im Fokus hybrider Kriegsführung**: Russland setzt gezielt Desinformation und Einschüchterungstaktiken ein, um die deutsche Unterstützung für die Ukraine zu untergraben. Dabei werden auch Unternehmen zum Ziel. Im Sommer 2024 wurde so beispielsweise bekannt, dass die russische Regierung die Entführung von Armin Papperger, Chef des Rüstungsunternehmens Rheinmetall mit Sitz in Düsseldorf, geplant haben soll. Darüber hinaus hat im Herbst 2025 ein russisches Bot-Netzwerk eine Desinformationskampagne verbreitet, dass die Ehefrau von Bundeskanzler Merz kurz vor dem Gewinn einer Ausschreibung Aktien des Unternehmens gekauft haben soll.*

Darüber hinaus besteht die Gefahr des Missbrauchs von Bewertungsportalen und Foren, die genutzt werden können, um mit gefälschten negativen Rezensionen das Image eines Unternehmens zu sabotieren. Vermehrt kann dafür auf fingierte Artikel oder Websites gesetzt werden. Länger anhaltende Desinformationskampagnen können so auch zu nachhaltigen Reputationsschäden und Vertrauensverlusten von wichtigen Stakeholdern führen.

Zu den relevanten Gefahren zählen gefälschte Social-Media-Profile, Dokumente und Mitteilungen, manipulative Narrative und koordinierte Bot-Kampagnen. Zunehmend sind Unternehmen insbesondere durch **KI-generierte Falschinformationen und Deepfakes** gefährdet, die mit erheblichen Geschäftsrisiken wie Finanzbetrug einhergehen können. Dazu gehört beispielsweise sogenannter "CEO-Fraud", bei dem Kriminelle mit geklonten Stimmen als vermeintlicher Chef Zahlungsanweisungen an Mitarbeitende geben. Eine internationale Befragung von PR-Expert:innen von Unternehmen zeigt zudem, dass fast 80 % Fake News und insbesondere Deepfakes für eine messbare **Gefahr für den Ruf ihres Unternehmens** halten oder bereits erfahren haben.

Übergreifend verschärft sich die **Cyberbedrohungslage** für Unternehmen vor dem Hintergrund von neuen technischen Möglichkeiten kontinuierlich. Der Gesamtschaden durch Cyberattacken an der deutschen Wirtschaft belief sich in dem zwölfmonatigen Erhebungszeitraum 2024 und 2025 erstmals auf über **200 Milliarden Euro**. 15 % der vom TÜV befragten Unternehmen verzeichneten so in den Jahren 2024 und 2025 IT-Sicherheitsvorfälle. Zugleich hat sich die Zahl der Hackerangriffe auf deutsche Unternehmen zwischen 2021 und 2024 vervierfacht.

Gleichzeitig zeigt sich eine ausgeprägte **Diskrepanz zwischen Selbstwahrnehmung und tatsächlicher Lage**: 91 % der Unternehmen bewerten ihre Cybersicherheit als effektiv. Demgegenüber sind laut Cisco Cybersecurity Readiness Index 2025 lediglich 32 % der Unternehmen gut oder sehr gut auf Cybergefahren vorbereitet, und nur 5 % gelten als optimal aufgestellt. Hinzu kommen **Fehleinschätzungen vieler kleiner und mittlerer Unternehmen** (KMU), die sich als "zu klein" für Angriffe wahrnehmen (66 %) oder ihre Daten als nicht interessant genug für Kriminelle sehen (63 %). Dabei sind KMU überproportional stark von Cyber-Erpressungsangriffen betroffen und gelten als **besonders verwundbar**.

Als zentrales Risiko und größte Schwachstelle gilt jedoch weiterhin **menschliches Fehlverhalten**. Dies entsteht oft aus **Überforderung**: Nur rund 25 % der Mitarbeiter:innen trauen sich zu, Phishing sicher zu erkennen, während 54 % ein Unsicherheitsgefühl beim Öffnen von Anhängen haben. Gleichzeitig ist **Phishing** die häufigste Angriffsmethode und betrifft 22 % der Unternehmen. Zunehmend wird auch der **Einsatz von Künstlicher Intelligenz in Cyberangriffen** und eine daraus resultierende vergrößerte Angriffsfläche befürchtet. 51 % der Unternehmen beobachten einen verstärkten Einsatz von KI-Systemen bei Angriffen, unter anderem in Form von Deepfakes und Robocalls.

Anfälligkeiten für Desinformation

Die Gesamtbedrohungslage muss dabei auch im Kontext individueller Anfälligkeitsmerkmale betrachtet werden. Zahlreiche wissenschaftliche Studien und Umfragen zeigen übereinstimmend, dass **psychologische Faktoren die zentralen Treiber für Verschwörungsglauben und Anfälligkeit gegenüber Desinformation** sind. Insbesondere Verschwörungsmentalität, politisches Misstrauen, Einsamkeit und gesellschaftliche Unzufriedenheit werden als stärkste Risikofaktoren identifiziert. Studien des Progressiven Zentrums sowie der Bertelsmann Stiftung belegen enge Zusammenhänge zwischen diesen Merkmalen und Verschwörungsglauben. Eine Weltanschauung, die von Verschwörungsglauben gekennzeichnet ist, sagt so die Anfälligkeit für Desinformation auch stärker vorher als beispielsweise politische Einstellungen oder Mediennutzung.

Relevant ist dennoch auch der **Einfluss politischer und ideologischer Identität**. Unabhängig von Alter und Bildung werden (Des-)Informationen als glaubwürdiger wahrgenommen, wenn sie mit der eigenen politischen Haltung übereinstimmen (siehe etwa Sultan et al. oder Bryanov et al.). Dies gilt insbesondere für **pro-russische Narrative**, denen Personen mit bestimmten parteipolitischen Präferenzen überdurchschnittlich häufig zustimmen.

Social Media wird ebenso als zentraler Verbreitungs- und Verstärkungsraum für Desinformation identifiziert. Insbesondere TikTok, X/Twitter, YouTube und Facebook erhöhen die Anfälligkeit der Nutzer:innen, während der **Konsum traditioneller Medien mit geringerer Desinformationsanfälligkeit einhergeht**. Da Jugendliche soziale Netzwerke besonders intensiv nutzen, kommen sie häufiger mit problematischen Inhalten in Kontakt (JIM-Studie 2024).

Auch sozioökonomische Faktoren spielen eine relevante Rolle. Mehrere Studien zeigen einen **Zusammenhang zwischen ökonomischer Benachteiligung**, etwa niedrigem Einkommen oder Arbeitslosigkeit, **und erhöhter Anfälligkeit für Desinformation und Verschwörungserzählungen** (z. B. Bertelsmann Stiftung oder Konrad-Adenauer-Stiftung). Insbesondere junge Erwachsene, die in ökonomisch prekären Umständen leben, gelten als Zielgruppe von Desinformationskampagnen.

Die Befunde zu Alter, Bildung und Geschlecht sind dagegen uneinheitlich. **Alterseffekte erweisen sich als inkonsistent oder gering**, wobei einzelne Studien ältere Menschen als kompetenter im Erkennen von Desinformation einschätzen, während andere Analysen diese Gruppe als besonders gefährdet beschreiben. Auch für die formale Bildung finden sich widersprüchliche Ergebnisse: Während in manchen Studien kein **Zusammenhang zwischen dem Bildungsniveau und der Wahrscheinlichkeit des Verschwörungsglaubens** einer Person festgestellt werden konnte, zeigen andere Untersuchungen einen solchen Zusammenhang auf: Ein höheres Bildungsniveau verringert demnach die Anfälligkeit für Verschwörungsglauben.

Regionale und gruppenspezifische Analysen ergänzen dieses Bild. Für Deutschland werden in mehreren Studien (etwa CeMAS und Friedrich-Naumann-Stiftung) höhere Zustimmungswerte zu bestimmten Narrativen in **Ostdeutschland** dokumentiert, während andere Untersuchungen keine Ost-West-Unterschiede finden. Zudem zeigen Studien, dass Menschen mit **Migrationshintergrund**, insbesondere mit russischem Hintergrund, sowie Personen mit religiöser oder spiritueller Orientierung häufiger bestimmten Desinformationsnarrativen zustimmen und diese seltener erkennen.

Bedarfe und Empfehlungen

Die Reaktionen von Unternehmen auf Desinformation und Bedrohungen im digitalen Raum haben derzeit mehrere Schwachstellen. Im Bereich der Desinformation stechen zwei Bedarfe hervor. Erstens wird **mehr Verständnis und Wissen über das Thema** an sich, über die relevanten Verbreitungswege und die technologischen Entwicklungen gefordert. Dazu gehört auch das Wissen darüber, welche Personengruppen aus welchen Gründen von Desinformation beeinflusst werden und wie individuelle und organisationsweite Resilienz gestärkt werden kann. Übergreifend gelten so Bildungsmaßnahmen zur **Steigerung der Medienkompetenz** und der **kritischen Reflexionsfähigkeit** als zentrale Faktoren für eine bessere Erkennung und Abwehr von Desinformation und digitalen Manipulationen.

Zweitens werden oftmals **fehlende strategische Mechanismen gegen Desinformation** bemängelt. Da Unternehmen in allen möglichen Geschäftsbereichen und auf allen Ebenen von Cyberattacken und Desinformation angegriffen werden können, ist auch eine **vollumfängliche Gegenstrategie** notwendig. In der Pflicht steht dabei besonders die Unternehmensführung. Durch eine kohärente Strategie kann ein Unternehmen dadurch sogar eine Vorbildfunktion nach außen einnehmen.

Potenzial besteht vor allem im Bereich Desinformation, da nur etwas mehr als die Hälfte der Unternehmen laut Institut der Deutschen Wirtschaft angibt, sich gegen Desinformation zu schützen und fast 20 % dies in Zukunft noch tun möchten. Die ergriffenen Maßnahmen im Bereich Cybersicherheit sind **zumeist schon proaktiv und nicht nur reaktiv**. Dennoch hinkt Deutschland im globalen Vergleich etwas hinterher: Während hierzulande lediglich 15 % deutlich mehr in proaktive Maßnahmen investieren, liegt der Wert global schon bei 24 %. Gleichzeitig geben 92 % der deutschen Unternehmen an, ihre **Cyberstrategie aufgrund der aktuellen Bedrohungslage anpassen zu wollen**.

Zweitens besteht zwischen den Unternehmenszielen und der **praktischen Umsetzung von Maßnahmen gegen Cyberangriffe und Desinformation** eine erhebliche Lücke: Während Schulungen von Mitarbeitenden und die Förderung einer konsequenten "Cyberhygiene" als besonders wirksame Schritte für Cyberresilienz gelten, bieten nur 24,4 % der Unternehmen **regelmäßige Trainings** in dem Bereich an. Gleichzeitig besteht ein genereller **Weiterbildungsbedarf im Bereich Cybersecurity**. Dies gilt insbesondere für kleine und mittlere Unternehmen mit einem anhaltenden Mangel an Cybersecurity-Fachkräften und an Ressourcen für Informationssicherheit. Vor diesem Hintergrund wird die **systematische Aus- und Weiterbildung der Mitarbeitenden** als zentral angesehen. Schulungen im Bereich Cybersicherheit entsprechen dabei auch dem Wunsch von einer Mehrheit der Beschäftigten.

Zur Steigerung der Akzeptanz von Sicherheitsmaßnahmen wünschen sich die Befragten zudem **vereinfachte Prozesse sowie eine direkte Ansprache im beruflichen Kontext**. Konkret stellen **Unkenntnis über interne Sicherheitsrichtlinien** oder eine Wahrnehmung von Maßnahmen als "zu kompliziert" Hürden dar. Darüber hinaus sind fehlende Kompetenzen im **Umgang mit neuen Bedrohungen durch KI** zu erkennen, insbesondere in Bezug auf die Sensibilisierung für KI-gestützte Angriffe sowie das Verständnis und die Erkennung von Deepfakes.

Quellen

AFP Faktencheck (2025). Behauptung über „Sitzhasen“ bei Lidl und Aldi ist irreführend

ALARM (2023). Game over vs. Game Lover - Serious Games als wirksame Security Awareness-Maßnahmen für KMU im Projekt “Alarm Informationssicherheit” - Framework mit Kommunikationsleitfaden, FAQ und Ausblick

Audit Committee Institute e.V. (2025). Quarterly - extra: Fake Futures oder das Ende der Realität

Bertelsmann Stiftung (2025). Verschwörungsglaube als Gefahr für Demokratie und Zusammenhalt. Erklärungsansätze und Prävention

Bitkom e. V. (2025). Russland und China nehmen deutsche Wirtschaft ins Visier

Bryanov, K., Vziatysheva V. (2021). Determinants of individuals’ belief in fake news: A scoping review determinants of belief in fake news

Buten un Binnen (2025). Shitstorm gegen Bremer Käsehersteller Milram wegen bunter Verpackungen

Capital (2025). Der falsche Bill: So wurde der Bayer-Chef Opfer eines Deepfakes

CeMAS – Center für Monitoring, Analyse und Strategie (2022). Belastungsprobe für die Demokratie: Pro-russische Verschwörungserzählungen und Glaube an Desinformation in der Gesellschaft

CHEQ (2019). The Economic Cost Of Bad Actors On The Internet

Cisco (2025). 2025 Cisco Cybersecurity Readiness Index

CyberSicher (2025). CyberSicher Lagebild 2025: Die aktuelle Bedrohungslage für kleine und mittlere Unternehmen in Deutschland

EY (2025). Datenklaustrudie 2025: Virtuelle Gefahr – reale Schäden

FORBES (2024). The Dark Side Of AI: How Deepfakes And Disinformation Are Becoming A Billion-Dollar Business Risk

Friedrich-Naumann-Stiftung für die Freiheit (2025). TikTok, X & Co. - Mediennutzung und die Anfälligkeit für Desinformation

Gartner (2025). Gartner Predicts 50% of Enterprises Will Invest in Disinformation Security and TrustOps by 2027

G DATA CyberDefense AG (2025). Cybersicherheit in Zahlen

heise (2024). Deepfake-Anruf: Lastpass-Mitarbeiter fällt fast auf Fake-CEO rein

IDW (2025). Fake News – Risiken und Handlungsbedarf für Gesellschaft, Unternehmen und Wirtschaftsprüfer.

IW (2026). IW-Trends. Die Rolle der Privatwirtschaft in der Gesamtverteidigung Deutschlands – Ergebnisse einer Unternehmensbefragung

Konrad-Adenauer-Stiftung (2020). Verschwörung in der Krise: Repräsentative Umfragen zum Glauben an Verschwörungstheorien vor und in der Corona-Krise

KPMG (2024). Der Einfluss von Desinformation auf Unternehmen.

Mastercard (2025). Mastercard Studie: Cyberbetrug gefährdet kleine und mittlere Unternehmen in Deutschland

Medienpädagogischer Forschungsverbund Südwest (mpfs) (2024). JIM-Studie 2024: Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger

Mishra, S. (2025). Misinformation and

Disinformation in the Digital Age: A Rising Risk for Business and Investors.

Orange Cyberdefense (2026). Security Navigator 2026

Progressives Zentrum (2023). Extrem einsam? Eine demokratische Relevanz von Einsamkeitserfahrungen unter Jugendlichen in Deutschland

PwC (2026). Digital Trust Insights 2026: Chancen und Risiken für deutsche Unternehmen

Stoica, S. E. (2024). Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law. Social and Demographic Determinants of Online Disinformation

Süddeutsche Zeitung (2025). Süßigkeiten: Ostern ade? Wie mit dem „Sitzhasen“ Stimmung gemacht wird

Sultan, M. et al. (2024). Susceptibility to online misinformation: A systematicmeta-analysis of demographic and psychological factors

Tagesschau (2024). Bericht über russischen Anschlagsplan auf Rheinmetall-Chef

The Notified Team (2024). How Deepfakes and Fake News Are Shaping Influence.

The Insider (2025). Germany plans €377B in defense procurements as Kremlin bot network spreads fake story about Chancellor Merz's wife buying Rheinmetall shares

TÜV-Verband (2025). Cybersicherheit in deutschen Unternehmen: Neue Bedrohungslage – besserer Schutz

Universität Bonn (2024). Fake News schaden der Wirtschaft

vbw (2026). Sicherer Umgang mit Desinformation

Vodafone Stiftung (2021). Studie zu Desinformation: Expert:innen sehen größte Gefahr für gesellschaftlichen Zusammenhalt und Radikalisierung

WirtschaftsWoche (2025). Milram-Käseverpackungen: Was heißt hier „woke“? Eine Debatte über Käse und Gesellschaft

World Economic Forum (2026). The Global Risks Report 2026 21st Edition

Zilinsky, J. et al. (2024). Justifying an Invasion: When Is Disinformation Successful?

Ziemer C. T. et al. (2024). Identity is key, but Inoculation helps – how to empower Germans of Russian descent against pro-Kremlin disinformation

KONTAKT

Die Analyse wurde im Auftrag der Staatskanzlei des Landes Nordrhein-Westfalen erstellt.

Stand: 04.02.2026

polisphere
[passion for politics]

polisphere GmbH | Chausseestr. 5, 10115 Berlin |
www.polisphere.eu | berlin@polisphere.eu | @polisphere

© polisphere GmbH, 2026, alle Rechte vorbehalten