

EXECUTIVE SUMMARY

Desinformationsangriffe gegen Unternehmen Studie 2026



Eine erneute Analyse von Complexium, Dr. Christopher Nehring und VSW-Bundesverband rund zehn Jahre nach der ersten gemeinsamen Studie zu Desinformationsangriffen zeigt:

Der Angriffsvektor ist heute deutlich bekannter, wird jedoch weiterhin nicht ausreichend berücksichtigt.

Dr. Nehring stellt anhand von aktuellen Beispielen dar, dass der „neue Cyberangriff“ schnell, billig und wirksam ist und auf die Vorstandsagenda gehört:

Desinformation ist „der neue Cyberangriff“ mit direktem Business-Impact

Weltwirtschaftsforum, Bitkom, Gartner oder der ehem. Chef des britischen Geheimdienstes ranken Desinformation unter die dringendsten globalen Gefahren für Sicherheit, Stabilität, Umsatz, Reputation, Talent, Lieferketten und Vertrauen. Der finanzielle Schaden liegt im zweistelligen Milliardenbereich. Deutsche Unternehmen beurteilen das Thema jedoch überwiegend als geringes bis mittleres Risiko und nehmen es nur zögerlich in Aktionspläne auf.

Desinformation ist billig, schnell, facettenreich, wirksam und schwer zu fassen

Geopolitische Krisen, gesellschaftliche Polarisierung und technologische Entwicklungen (KI) begünstigen Angreifer. Beispiele reichen von russischen Einflussoperationen, chinesische Kampagnen, Cyber-Kriminellen und politischen Aktivisten. Besonders betroffene Branchen in Deutschland sind die Automobilindustrie, der Energiesektor, Rüstung und Zulieferer sowie Unternehmen mit klarer politischer Positionierung.

Desinformation gehört wie Cybersecurity auf die C-Level-Agenda: Governance, Lagebild, Playbooks, Übungen.

- Klarer Owner/SPOC (Task Force)
- 360° Monitoring/OSINT & Threat Intelligence
- Incident-Response für Informationsangriffe
- vorgefertigte Kommunikationsbausteine
- realistische Legal/Takedown-Strategie
- Simulationen/Red-Teaming
- Kooperation mit Plattformen/Behörden.

Aus der Erhebung des VSW-Bundesverbandes lassen sich drei Forderungen an unterschiedliche Adressaten ableiten:

Zusammenarbeit ist auch hier der Schlüssel zum Erfolg

Sei es im Unternehmen durch gemeinsame Task-Forces der involvierten Abteilungen oder zwischen staatlichen und wirtschaftlichen Stakeholdern. Desinformation ist eine Querschnitts-Gefahr und muss als solche auch behandelt werden.

Plattformbetreiber müssen Verantwortung tragen und schnelle sowie einfache Gegenmaßnahmen bereitstellen.

Die sich rasch entwickelnden Technologien dürfen nicht nur zum Vorteil der Angreifer sein. Rechtliche Rahmenbedingungen sowie technologische Lösungen müssen zum Kampf gegen Desinformation weiterentwickelt werden.

Awareness zur Desinformation muss sowohl in Unternehmen als auch in der breiten Öffentlichkeit viel intensiver angegangen werden

Eine breit angelegte Kampagne ist nötig, um Mitarbeiter und Bevölkerung zu sensibilisieren und die Gefahr für alle Akteure zu minimieren.



Zur Studie:

Ausgehend von der Vermutung, dass die bisherige Reaktionszurückhaltung von einem Gegner durchaus gewollt sein kann, skizziert Prof. Dr. Martin Grothe ein Rahmenmodell für ein Lagebild „Hybride Angriffe“ mit einer grundlegenden Struktur dieser Angriffe sowie KI-Szenarien mit konkreten Mitigationsmaßnahmen:

Unternehmen als strategische Angriffsziele

Desinformationsangriffe gegen Unternehmen sind oftmals keine isolierten Phänomene, sondern dienen als erste Angriffsstufe in einem hybriden Gesamtrahmen. Entlang von vier strategischen Stufen ist es Ziel,

- durch die Schwächung von Unternehmen ein Grundmisstrauen aufzubauen,
- dann eigene, d.h. gegnerische Positionen zu verfestigen,
- um dies in politischer Beeinflussung von Wahlkämpfen und
- später Regierungshandeln zu kapitalisieren.

Vierstufige Eskalationslogik (TEAM):

Systematische Kampagnen folgen oftmals einer operativen Skala:

- Thematisierung (Schaffung von Narrativen),
- Emotionalisierung (Appell an Angst/Wut),
- Aktivierung (Aufruf zur Interaktion) und schließlich
- Mobilisierung, bei der die Kampagne in reale Aktionen wie Boykotte, Proteste oder Wahlentscheidungen übergeht.

Angriffsstufen und Eskalationskala können Dimensionen in einem Lagebild "Hybride Angriffe" aufspannen.

Herausforderung der Detektion

Da Angriffe oft dekontextualisierte, aber faktisch korrekte Informationen nutzen, ist eine Erkennung schwierig. Sie gelingt nur auf einer höheren Ebene durch die laufende Analyse großer Datenmengen auf Auffälligkeiten, atypische Muster, Themenpeaks, besondere Akteursfunktionen sowie Qualifizierung durch Analysten.

KI-gestützte Früherkennung (PrediCX)

Mithilfe eines prädiktiven Systems können aus einer breiten Datenbasis (Social Media, Telegram, News sowie verdichteten Sicherheitsberichten und Factbooks) frühzeitig spezifische Bedrohungsszenarien generiert werden. Dies ermöglicht es Unternehmen, im Rahmen von Digital Listening „vor die Lage“ zu kommen und Angriffe mitunter in der Entstehungsphase zu erkennen.

Mitarbeitende als „intelligente Sensoren“

Eine entscheidende Maßnahme zur Stärkung der Resilienz ist neben vorbereitenden Wargames und einem laufenden Monitoring die Einbindung der Belegschaft. Sensibilisierte Mitarbeitende fungieren als Sensoren, die Angriffe frühzeitig erkennen und so nicht nur die Reputation des Unternehmens schützen, sondern auch die gesellschaftliche Widerstandskraft stärken.

Wir laufen Gefahr, diese Bedrohung nicht ernst genug zu nehmen. Desinformationsangriffe zielen auf mehr als die Reputation. Auch Destabilisierung ist kein finales Ziel. Schwierigkeiten der Detektion und der Schadensmessung dürfen die aktive Auseinandersetzung nicht verhindern.

Zur Studie:

