

IW-Kurzbericht Nr. 60/2026

Hybride Bedrohungen treffen deutsche Unternehmen

Simon Gerards Iglesias / Dan Muncaster / Edgar Schmitz, 05.09.2026

Ob Drohnenangriffe, Anschläge auf die Energieinfrastruktur oder Desinformationskampagnen: Hybride Angriffe sind bei deutschen Unternehmen angekommen. In einer Unternehmensbefragung des Instituts der deutschen Wirtschaft berichten fast ein Fünftel aller befragten Unternehmen, dass sie in der jüngeren Vergangenheit durch hybride Bedrohungen ausländischer Akteure starke oder sehr starke Auswirkungen gehabt haben.

Die jüngst erfolgten oder versuchten Anschläge auf Energieinfrastrukturen in Deutschland sowie der versuchte Drohnenangriff am Flughafen Leipzig haben die Debatte über die Anfälligkeit Deutschlands für hybride Kriegsführung entfacht. Die Bundesregierung ordnete den Vorfall in Leipzig am 1. September 2026 nach einigen Tagen polizeilicher und nachrichtendienstlicher Ermittlungen Russland zu (ZDF, 2026). Die Ermittlungen zu den beiden anderen Angriffen in Brandenburg und Bergheim erweisen sich als schwierig. Die Vorfälle stehen damit exemplarisch für ein sicherheitspolitisches Problem in Deutschland: Die Zuordnung der Verantwortlichen für Angriffe wie Sabotageakte bleibt häufig schwierig. Zugleich handelt es sich bei der Beteiligung ausländischer Kräfte um eine Form des Angriffs unterhalb der Schwelle eines militärischen Krieges, die erhebliche Sicherheitsrisiken birgt und beträchtliche wirtschaftliche Kosten sowie gesellschaftliche Folgeschäden verursachen kann.

Unternehmen als hybride Zielscheibe

Der Begriff „hybride Bedrohungen“ bezeichnet schädliche Aktivitäten, die mit böswilliger Absicht von staatlichen oder nichtstaatlichen Akteuren geplant und durchgeführt werden (Hybrid Centre of Excellence, o.J.). Häufig werden dabei Cyberangriffe, wirtschaftlicher Druck, verdeckte politische Einflussnahme, Desinformation oder militärische Aktionen kombiniert.

Neu ist auch die Rolle, die Unternehmen in diesem Kontext spielen: Unternehmen waren bereits vor der aktuellen geopolitischen Konfrontation Ziele von Spionage, Sabotage und Erpressung. Für das Jahr 2025 wird der Schaden für deutsche Unternehmen auf 289 Milliarden Euro geschätzt (Bitkom, 2025). Rund 70 Prozent des Gesamtschadens entfielen dabei auf Cyberangriffe. Auch die Angaben zur Herkunft der Angriffe weisen auf eine geopolitische Konzentration hin. Von den betroffenen Unternehmen konnten jeweils 46 Prozent mindestens einen Angriff bis nach Russland beziehungsweise China zurückverfolgen. Rund ein Drittel konnte die Angriffe keiner eindeutigen Quelle zuordnen. Der Befund weist damit darauf hin, dass Russland und China auch für deutsche Unternehmen die zentralen ausländischen Gefahrenpunkte darstellen.

Hybride Bedrohungen treffen viele Unternehmen

Anteil der Unternehmen, die sich durch hybride Bedrohungen aus dem Ausland „eher stark“ oder „sehr stark“ betroffen sehen – nach Branche und Unternehmensgröße, in Prozent

Unternehmensgröße



Branchen



N = 1.041

Quelle: IW-Zukunftspanel, Welle 54, 2026, Institut der deutschen Wirtschaft

Früher lagen die Motive häufig in der Beschaffung von Technologien, der Ausspähung von Geschäftsgeheimnissen oder der unmittelbaren finanziellen Bereicherung. Heute geraten Unternehmen zunehmend ins Visier politischer Akteure, die im Rahmen hybrider Kriegsführung gegen sie vorgehen: Unternehmen bilden zentrale Knotenpunkte in der Energieversorgung, Logistik, Kommunikation, Gesundheitsversorgung und industriellen Produktion. Ein Angriff auf ein Unternehmen kann deshalb über den unmittelbaren wirtschaftlichen Schaden hinaus die Versorgungssicherheit beeinträchtigen, politische Entscheidungsprozesse beeinflussen oder das Vertrauen in die staatliche Handlungsfähigkeit schwächen.

Fast ein Fünftel der Unternehmen betroffen

Eine aktuelle Befragung im IW-Zukunftspanel zeigt:

- Fast ein Fünftel der befragten Unternehmen berichtet von starken oder sehr starken Auswirkungen hybrider Bedrohungen, wie Cyberangriffen, Desinformation, Spionage oder Sabotage, durch ausländische Akteure.
- Bei mittelgroßen Unternehmen (50 bis 249 Beschäftigten) liegt der Anteil bei 27 Prozent, bei großen Unternehmen ab 250 Beschäftigten bei 39 Prozent.

- Besonders betroffen sind Unternehmen aus dem Bereich der Energie- und Wasserversorgung, der Informations- und Kommunikationswirtschaft sowie wirtschaftsnahe Dienste (z.B. Labore oder Unternehmensberatungen).

Die neuen Daten zeigen, dass hybride Bedrohungen aus dem Ausland bereits von zahlreichen Unternehmen wahrgenommen werden. Besonders stark betroffen sind Unternehmen, die kritische Infrastrukturen betreiben, wie Informations- und Kommunikationstechnik (IKT) oder Energie- und Versorgungsunternehmen. Die Ergebnisse verdeutlichen, dass politische Motive bei hybriden Angriffen heute eine größere Relevanz haben. Dies erfordert eine neue Abwehrbereitschaft.

Betriebliche und politische Abwehr

Bei der Abwehr hybrider Angriffe waren Unternehmen in der Vergangenheit nicht untätig. Die Befragungsergebnisse zeigen, dass ein hoher Anteil der Unternehmen auf geopolitisch motivierte Risiken mit erhöhten Investitionen in die IT-Sicherheit und die digitale Infrastruktur reagiert hat. Allerdings bleiben Unternehmen anfällig: Nur ein kleinerer Teil gibt an, verstärkt in die Absicherung seiner Energieversorgung investiert zu haben. Eine Mehrheit der Unternehmen verfügt über keine Notfallpläne für den Umgang mit dem Ausfall kritischer Infrastrukturen.

Ein großes Problem besteht zudem darin, dass sich der überwiegende Teil der Unternehmen nicht mit Sicherheitsbehörden über mögliche Gefahren, Notfallpläne

und Strategien austauscht. Zudem verfügen über 46 Prozent der Großunternehmen im verarbeitenden Gewerbe nicht über einen wirksamen Werkschutz. Stärker ausgeprägt ist hingegen der Schutz vor Desinformation und Spionage; 44 Prozent beziehungsweise 63 Prozent dieser Unternehmensgruppe haben hierfür entsprechende Vorkehrungen getroffen (Bardt et al., 2026). Die mangelnde Vorbereitung und die hohe Gefahrenexposition stellen eine Gefahr für die Funktionsfähigkeit von Wirtschaft und Gesellschaft dar.

Politische Implikationen

Das KRITIS-Dachgesetz ist im März 2026 in Kraft getreten. Es verpflichtet Unternehmen und Betreiber kritischer Infrastrukturen zu zusätzlichen Meldungen und Risikoanalysen. Damit schafft das Gesetz einen wichtigen rechtlichen Rahmen für den Schutz kritischer Infrastrukturen. Gemessen an der tatsächlichen Bedrohungslage bleibt es jedoch hinter den Erfordernissen zurück. Die Abstimmungswege bleiben durch Zuständigkeitsschwierigkeiten zwischen Bund und Ländern diffus und unklar. Die Umsetzung wird durch umfangreiche sowie uneinheitliche Regelungen erschwert. Dies gilt insbesondere dort, wo Länderregelungen unterschiedliche Schwellenwerte zur Definition der kritischen Infrastruktur ansetzen.

Die hybriden Bedrohungen sind Teil einer neuen gesamtgesellschaftlichen Risikolage. Sie gehen zunehmend von ausländischen staatlichen Akteuren aus, deren Abwehr primär eine staatliche Aufgabe ist.

Die Politik muss deshalb die Fähigkeiten zur Abwehr und Aufklärung hybrider Angriffe ausbauen und darf zusätzlichen Schutz nicht primär Unternehmen anlasten. Vielmehr kann ein verbessertes KRITIS-Gesetz sowie die Reform der Nachrichtendienste, die ihnen zusätzliche Befugnisse verschafft, die staatliche Abwehrfähigkeit erhöhen. Eine wirksame Sicherheitsstrategie muss zudem nicht nur in der Lage sein, Angriffe abzuwehren, sondern auch mit drohenden Sanktionen abschrecken. Die schnelle Reaktion der Bundesregierung nach dem Vorfall am Leipziger Flughafen ist daher begrüßenswert.

Die Bedrohung durch hybride Angriffe betrifft Unternehmen unmittelbar. Angriffe verursachen erhebliche Kosten, erhöhen die Unsicherheit und können im schlimmsten Fall zu Produktionsausfällen führen. Der

Schutz kritischer Infrastrukturen ist deshalb nicht allein eine sicherheitspolitische Aufgabe. Wirtschaftssicherheit entwickelt sich zunehmend zu einem eigenständigen Standortfaktor. Für Unternehmen wird damit entscheidend, wie verlässlich und effektiv der Staat seine Aufgabe der Verteidigung von hybriden Bedrohungen wahrnimmt und wie eng verzahnt sie mit den unternehmerischen Sicherheitsstrategien ist.

Quellen

Bardt, Hubertus / Gerards Iglesias, Simon / Radunz, Alexander / Röhl, Klaus-Heiner, 2026, Die Rolle der Privatwirtschaft in der Gesamtverteidigung Deutschlands, IW-Trends, Nr. 4, Köln

Bitkom, 2025, Russland und China nehmen deutsche Wirtschaft ins Visier, 18.09.2025, [LINK](#), [03.09.2026]

Hybrid CoE, o.J., Hybrid threats as a concept, [LINK](#), [03.09.2026]

ZDF, 2026, Drohnen-Vorfall: Bundesregierung macht Russland verantwortlich, 01.09.2026, [LINK](#), [03.09.2026]