Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 02/2026 | 23. Juli 2026

Betreff | Sicherheits- und Verteidigungsbranche als Zielfläche

Ausgangslage

Die Sicherheits- und Verteidigungswirtschaft steht traditionell besonders im Fokus sowohl von ausländischen Nachrichtendiensten als auch von extremistischen Akteuren. Die russische Vollinvasion in der Ukraine und das dynamische Konfliktgeschehen im Nahen und Mittleren Osten erhöhen die Gefährdungslage. Das gilt mit Blick auf die strategische Aufklärung, die verdeckte Beschaffung von militärischen Technologien und einschlägigem Know-how, aber auch gezielte Einflussnahme und Sabotagehandlungen.

Sachverhalte

Unternehmensliste des RUS Verteidigungsministeriums

In den Medien kursierte im April 2026 eine Liste des russischen Verteidigungsministeriums mit 21 europäischen Unternehmen, denen vorgeworfen wird, mit der Produktion und Lieferung von Drohnen für die Ukraine in Verbindung zu stehen. Die Liste enthielt u. a. die Namen von drei Unternehmen mit Sitz in Deutschland. Der stellvertretende Vorsitzende des Sicherheitsrates der Russischen Föderation, Dmitrij Medwedew, hat diese Unternehmen in einem Beitrag auf der Plattform „X“ zu potenziellen Zielen für die russischen Streitkräfte erklärt.

Festnahmen wegen Verdacht auf geheimdienstliche Agententätigkeit

Die Bundesanwaltschaft hat im März und April 2026 mehrere Personen wegen mutmaßlicher geheimdienstlicher Agententätigkeit festnehmen lassen. Dem kasachischen Staatsangehörigen Sergej K. wird zur Last gelegt, seit Mai 2025 von Deutschland aus fortlaufend in Kontakt zu einem russischen Geheimdienst gestanden und seinem Führungsoffizier u. a. Informationen über die militärische Unterstützung Deutschlands für die Ukraine sowie über die deutsche Sicherheits- und Verteidigungswirtschaft geliefert zu haben – insbesondere zu Unternehmen, die Drohnen und Roboter entwickeln. K. leitete wiederholt Fotos von öffentlichen Gebäuden in Berlin oder von militärischen Konvois auf Autobahnen weiter. Zudem informierte er seinen Kontaktmann beim Geheimdienst über geeignete Sabotageobjekte in Deutschland und bot an, weitere Personen für eine Sabotage-

und Spionagetruppe zu rekrutieren. Der rumänischen Staatsangehörigen Alla S. und dem ukrainischen Staatsangehörigen Sergey N. wird vorgeworfen, im Auftrag eines russischen Geheimdienstes eine Person in Deutschland ausgespäht zu haben, deren Firma von Deutschland aus Drohnen und dazugehörige Bauteile in die Ukraine liefert. Dazu sammelte N. im Internet Informationen und fertigte Filmaufnahmen vom Arbeitsplatz des Betroffenen an. Als N. nach Spanien verzog, übernahm S. seinen Auftrag. Sie begab sich zur Meldeanschrift der Zielperson und filmte die Örtlichkeit mit dem Mobiltelefon. Die Ausspähaktionen dienten mutmaßlich der Vorbereitung weiterer geheimdienstlicher Operationen gegen die Zielperson.

Kamerafund am Bahnhof in Minden

Die Staatsanwaltschaft Dortmund informierte im April 2026 über zwei Durchsuchungsmaßnahmen in Detmold und Bad Salzuflen. Hintergrund ist ein Strafverfahren wegen des Tatverdachts der Agententätigkeit zu Sabotagezwecken gegen einen litauischen Staatsangehörigen. Er wird mit einer Kamera in Verbindung gebracht, die im September 2025 auf einem Lichtmast am Bahnhof in Minden entdeckt wurde. In der Nähe des Bahnhofs ist mit dem deutsch-britischen Pionierbrückenbataillon 130 eine hochspezialisierte Einheit stationiert, die über das einzige Schwimmbrückensystem M3 innerhalb der NATO verfügt.

Bahnsabotage durch RUS Agenten in Polen

Polnische Behörden machen mehrere ukrainische Staatsangehörige für einen Sprengstoffanschlag im November 2025 auf eine der wichtigsten polnischen Bahnrouten für Hilfslieferungen und Militärtransporte in die Ukraine verantwortlich. Sie sollen im Auftrag Russlands gehandelt haben. Ende 2023 wurden in Polen bereits 16 Mitglieder eines russischen Agentenrings (zwölf ukrainische, drei belarussische und ein russischer Staatsangehöriger) zu Gefängnisstrafen bis zu sechs Jahren verurteilt. Sie hatten gestanden, mit ferngesteuerten Kameras u. a. Bahntransporte in Richtung Ukraine ausgespäht zu haben mit dem Ziel, einen Zug entgleisen zu lassen.

Phishing-Angriffe über Messenger-dienste

Ein wahrscheinlich staatlich gesteuerter Cyberakteur führt seit Frühjahr 2026 Phishing-Angriffe über Messengerdienste wie „Signal“ gegen hochrangige Ziele aus verschiedensten Bereichen durch. Partnerländer ordnen die Kampagne Russland zu. Auch Unternehmen und Personen aus der Sicherheits- und Verteidigungswirtschaft zählen zur Zielfläche des Akteurs. Charakteristisch für die Kampagne ist, dass weder Schadsoftware eingesetzt noch technische Schwachstellen der Messengerdienste ausgenutzt werden. Stattdessen bedienen sich die Angreifer legitimer Sicherheitsfunktionen der Anwendungen und kombinieren diese mit Social Engineering. Ziel ist es, unbemerkt Zugriff auf Einzel- und Gruppenchats sowie auf Kontaktlisten der betroffenen Personen zu erlangen. Details zu den erkannten Vorgehensweisen sind z. B. dem Gemeinsamen Sicherheitshinweis 01/2026 des BfV und des BSI zum „Phishing über Messengerdienste“ vom 6. Februar 2026 zu entnehmen.

Onlinehandel mit Standortdaten

Unter dem Mantel „Databroker Files“ recherchiert ein internationales Medienkollektiv bereits seit Anfang 2024 zum Datenhandel der Online-Werbeindustrie. Dem Team liegen nach eigenen Angaben Standortdaten von Millionen Menschen aus der ganzen Welt vor. Darunter sollen Hunderttausende Datenpunkte aus der Ukraine sein, wo Unternehmen der deutschen Sicherheits- und Verteidigungswirtschaft seit Beginn der russischen Vollinvasion verstärkt engagiert sind. In Deutschland selbst hat die Recherche sogar gezielt Personen ausfindig gemacht, die an bekannten Standorten großer Unternehmen der Branche ein- und ausgehen und deren Daten online zum Kauf angeboten werden. Die entsprechenden Probedatensätze allein sollen bereits genügen, um Arbeitswege, Wohnorte und Bewegungsprofile ableiten zu können.

Sanktionsumgehung zur Beschaffung von Rüstungsgütern für Russland

Im Februar 2026 hat die Bundesanwaltschaft in Lübeck und im Kreis Herzogtum Lauenburg fünf mutmaßliche Mitglieder (zwei deutsche, einen deutsch-ukrainischen und zwei deutsch-russische Staatsangehörige) einer kriminellen Vereinigung für Exportgeschäfte unter Verstoß gegen das Außenwirtschaftsgesetz (vorläufig) festnehmen lassen. Spätestens seit Beginn der russischen Vollinvasion sollen die Beschuldigten das Lübecker Handelsunternehmen des Angeklagten Nikita S. genutzt haben, um zu zahlreichen Gelegenheiten konspirativ Güter für die russische Industrie zu beschaffen und nach Russland auszuführen. Zur Verschleierung der Geschäfte bedienten sich die Beschuldigten mindestens einer weiteren Scheinfirma in Lübeck, Scheinabnehmern in und außerhalb der Europäischen Union sowie eines russischen Unternehmens als Empfänger, für das Nikita S. ebenfalls in verantwortlicher Position tätig ist. Ziel des Vorgehens war die Umgehung von Embargobestimmungen der Europäischen Union (Russland-Embargo-Verordnungen). Zu den Endabnehmern der ausgeführten Güter gehörten mindestens 24 gelistete Rüstungsunternehmen in Russland.

Propalästinensisch motivierte Angriffe gegen ISR Unternehmen

Aktivisten des deutschen Ablegers von „Palestine Action“ (PA) sind im September 2025 in das Gebäude des israelischen Unternehmens „Elbit Systems“ in Ulm eingedrungen und haben dieses mit Rauchbomben, Farbbeuteln sowie Graffiti attackiert. In der Folge wurden fünf Personen festgenommen, die sich seitdem in Untersuchungshaft befinden. Bei PA handelt sich um ein internationales Netzwerk aus dem säkularen propalästinensischen Extremismus, das sich 2020 in Großbritannien gründete und mittlerweile Ableger in mehreren europäischen Staaten hat. Als Ziel hat sich die Kampagne die Beendigung der aus ihrer Sicht gegebenen „Apartheid“ in Israel gesetzt. Die ebenfalls an der Aktion beteiligte Kampagne „Shut Elbit Down“ will verhindern, dass Waffen und Munition aus Ulm an die israelische Armee geliefert werden. PA beging in der Vergangenheit bereits europaweit eine Vielzahl von Vandalismus-Aktionen gegen Unternehmen, die in Verbindung mit dem Staat Israel stehen. Auf einer Website aus den PA-Milieu findet sich ein Link zur einer weltweiten „Target Map“.

Mutmaßlich linksextremistisch motivierte Karten mit Unternehmensstandorten

Verschiedene mutmaßlich linksextremistisch motivierte Websites bieten frei zugänglich entweder direkt oder verlinken (teils interaktive) Karten, die Standorte von Unternehmen der Sicherheits- und Verteidigungswirtschaft einschließlich (angeblicher) Zulieferer abbilden. Darüber hinaus listen sie auch „militaristische Lobbygruppen“ und andere Unternehmen auf, die (angeblich) für die Branche tätig sind.

Bewertung

Erhöhte Gefährdung durch RUS Spionage und Sabotage

Bundeskanzler Friedrich Merz und der ukrainische Präsident Wolodymyr Selenskyj haben sich Ende März 2026 im Rahmen der deutsch-ukrainischen Regierungskonsultationen darauf verständigt, die Zusammenarbeit u. a. im sicherheitspolitischen Bereich zu vertiefen. Die Veröffentlichung der Unternehmensliste durch das russische Verteidigungsministerium dürfte in erster Linie als Reaktion darauf zu verstehen sein. Dessen ungeachtet ist die Gefährdungslage für Unternehmen der Sicherheits- und Verteidigungswirtschaft in Deutschland, insbesondere solche, die mit der Ukraine kooperieren, weiterhin hoch. Die jüngsten Festnahmen durch die Bundesanwaltschaft verdeutlichen: Es besteht eine erhöhte Wahrscheinlichkeit, dass entsprechende Unternehmen das Ziel von Ausspähungs- und Sabotagehandlungen durch russische staatliche Stellen oder in deren Auftrag werden. Abhängig vom weiteren Kriegsverlauf sind selbst gezielte Angriffe gegen Einzelne (insbesondere Beschäftigte auf der Leitungsebene) nicht auszuschließen.

Militärische Einrichtungen und UKR-Logistikkette als Hochwertziele

Militärische Einrichtungen sind für ausländische Nachrichtendienste von besonderem Interesse. Die in Minden gefundene Kamera war in der Nähe des dort stationierten deutsch-britischen Pionierbrückenbataillons installiert. Es erscheint denkbar, dass die Installation der Kamera den Zweck verfolgte, hierüber Informationen zu erlangen. Die teilweise erfolgreich durchgeführten Bahnsabotageakte in Polen sind ein Beleg dafür, dass auch die militärische Logistikkette für die Nachschubversorgung der Ukraine ein herausgehobenes Ziel für russische Spionage und Sabotage ist. Russische Nachrichtendienste greifen dabei verstärkt auf sogenannte Low-Level-Agenten zurück. Dabei handelt es sich um ungeschulte nachrichtendienstliche Amateure, die für vergleichsweise geringe Bezahlung über Messengerdienste für einzelne Aufträge angeworben werden und häufig einen (klein)kriminellen Hintergrund aufweisen.

Hohes Gefährdungspotenzial durch Social Engineering

Die Phishing-Kampagne über Messengerdienste wie „Signal“ verdeutlicht das hohe Gefährdungspotenzial, das auch von vergleichsweise simplem Social Engineering ausgeht. Zudem verleitet die Nutzung scheinbar sicherer Messenger das Opfer dazu, die vorliegenden Angriffsvektoren nur unzureichend zu beachten, da Betroffene sich in einer falschen Sicherheit wiegen. Doch ausländische Nachrichtendienste finden laufend neue Wege, um die „Schwachstelle Mensch“ als Einfallstor für Angriffe zu nutzen. Umso wichtiger sind zielgerichtete Sensibilisierungen für neue Modi Operandi und regelmäßige Schulungen zum

sicheren Umgang mit Informations- und Kommunikationstechnik, insbesondere in sensiblen Branchen wie der Sicherheits- und Verteidigungswirtschaft.

Möglichkeit der Nutzung von Standortdaten für Anbahnungs- und Angriffszwecke

Der Verkauf und die Verbreitung von Standortdaten und daraus abzuleitenden Bewegungsprofilen stellen grundsätzlich einen schwerwiegenden Eingriff in die Privatsphäre dar. Insbesondere bei Personen mit Bezügen zu sensiblen Branchen wie der Sicherheits- und Verteidigungswirtschaft besteht eine erhöhte Gefährdung, dass ausländische Nachrichtendienste und andere sicherheitsgefährdende Akteure sich diese gezielt für Anbahnungs- und (möglicherweise auch physische) Angriffszwecke beschaffen und zunutze machen. Besondere Vorsicht ist bei Aufenthalten im Ausland geboten. Gerade in Staaten mit besonderen Sicherheitsrisiken (sogenannte SmbS) haben die Behörden teilweise weitreichende Befugnisse. Deren Nachrichtendienste können nach dortigem Recht legal Zugriff auf den Internet- und Mobilfunkverkehr haben, Daten abfangen und kontrollieren. Zudem können insbesondere auch staatliche Akteure Mobilfunkgeräte aus der Ferne kompromittieren und auslesen.

Immer neue Mittel und Wege zur Umgehung von Sanktionen

Hinter dem Netzwerk zur Sanktionsumgehung bei der Beschaffung von Gütern für die russische Rüstungswirtschaft stehen auf russischer Seite mutmaßlich staatliche Stellen. Es ist davon auszugehen, dass diese weiter immer neue Mittel und Wege suchen und einsetzen werden, um bestehende Sanktionen zu unterlaufen und Material und Know-how zu beschaffen, das für die Aufrechterhaltung der Kriegsanstrengungen benötigt wird, in Russland jedoch nicht produziert wird bzw. vorliegt.

Möglichkeit weiterer propalästinensischer Aktionen

Abhängig von der weiteren Entwicklung der Konfliktlage im Nahen und Mittleren Osten muss mit weiteren Aktionen propalästinensischer extremistischer Akteure gegen Unternehmen der Sicherheits- und Verteidigungswirtschaft in Deutschland gerechnet werden. Das gilt insbesondere für Unternehmen, die einen Bezug zu Israel haben, indem sie z. B. die israelischen Streitkräfte beliefern.

Besonders hohes linksextremistisches Mobilisierungspotenzial durch Antimilitarismus

Antimilitarismus ist traditionell ein wichtiger Begründungszusammenhang für linksextremistische Akteure. Seit der russischen Vollinvasion in der Ukraine und seit der Eskalation des Nahostkonflikts infolge der Anschläge der HAMAS vom 7. Oktober 2023 auf Israel sowie angesichts der jüngsten Waffengänge Israels und der USA gegen den Iran stehen die Sicherheits- und Verteidigungswirtschaft und ihre Zulieferer zusätzlich im Fokus. Das Aktionsfeld Antimilitarismus bietet vor dem Hintergrund der aktuellen Debatten über die „Kriegstüchtigkeit“ Deutschlands und über seine sicherheits- und verteidigungspolitische Rolle in einer sich neu ordnenden Welt ein besonders hohes Mobilisierungspotenzial für die linksextremistische Szene. Gewaltorientierte linksextremistische Akteure halten es für legitim, Unternehmen der Branche und ihre Zulieferer sowie die Bundeswehr zu schädigen, um eine angebliche „Militarisierung der Gesellschaft“ zu bekämpfen.

Handlungsempfehlungen

Maßnahmen für (IT-)Sicherheitsverantwortliche:

- Etablieren Sie ein ganzheitliches Risikomanagement, das physische Sicherheit, Informations- und Cybersicherheit sowie organisatorische Maßnahmen integriert und regelmäßig anhand der aktuellen Bedrohungslage überprüft wird.
- Sensibilisieren und schulen Sie Ihre Mitarbeitenden regelmäßig mit Blick auf aktuelle Gefahren durch ausländische Nachrichtendienste und – aufgrund ihrer aggressiven Vorgehensweisen – insbesondere durch die Nachrichtendienste Russlands.
- Informieren Sie im Rahmen der Prävention gezielt über Szenarien physischer Sabotagehandlungen sowie darüber, dass diese mit Cyberangriffen abgestimmt sein können. Berücksichtigen Sie dabei vorrangig Prozesse und Anlagen, deren Ausfall weitreichende und langanhaltende Schäden verursachen kann.
- Überprüfen Sie bestehende und geplante Veröffentlichungen (z. B. Lagepläne, Referenzprojekte) kritisch im Hinblick auf deren Nutzen für potenzielle Angreifer. Hinterfragen Sie insbesondere Veröffentlichungen, die über das gesetzlich erforderliche Maß hinausgehen, unterlassen Sie diese im Zweifel und nutzen Sie gesetzliche Ausnahmeregelungen von Transparenzpflichten. Geben Sie sensible Inhalte restriktiv nur an einen auf das notwendige Minimum beschränkten Personenkreis heraus („Need-to-know"-Prinzip), sofern keine Veröffentlichungspflichten entgegenstehen.
- Führen Sie in geeigneten Abständen Penetrationstests durch, um ein Feedback zum Umsetzungsstand der IT-Sicherheit aus Angreifer-Sicht zu erhalten. Sorgen Sie dafür, dass interne Dienste grundsätzlich nicht ohne Weiteres aus dem Internet erreichbar sind. Es bietet sich an, einen Zugriff lediglich aus dem Unternehmensnetzwerk oder über Virtual Private Network (VPN) zuzulassen.
- Prüfen Sie, inwieweit eine konsequente Netzsegmentierung und – wo sinnvoll – eine Verschleierung eigener IP-Adressbereiche durch Reseller dazu beitragen kann, Aufklärungsaktivitäten und automatisierte Angriffe auf kritische Systeme zu erschweren.

  Mehr dazu in unseren Informationsblättern zum Wirtschaftsschutz „Schutz vor Phishing", „Methoden der Spionage – HUMINT", „Schutz vor Sabotage".*

Maßnahmen für Personalverantwortliche:

- Wägen Sie bei Stellenausschreibungen kritisch ab, welche Informationen zwingend veröffentlicht werden müssen, um qualifiziertes Personal anzusprechen. Beschreiben Sie hierbei möglichst generische

Anforderungen. Verzichten Sie nach Möglichkeit auf Details zu konkreter Systemarchitektur und eingesetzter Technik.

- Stellen Sie in Ihrer Social-Media-Policy sicher, dass Beschäftigte Zurückhaltung bei Bezügen zum Unternehmen und Einsatzbereich üben. Falls keine solche Policy existiert, prüfen Sie eine Einführung.

Maßnahmen für Vertriebsverantwortliche:

- Nehmen Sie Kontakt zu uns auf, wenn Ihnen verdächtige Beschaffungsanfragen auffallen.

  Mehr u. a. zu möglichen Indizien für illegale Beschaffungsaktivitäten in unserem Informationsblatt zum Wirtschaftsschutz „Proliferation und Sanktionsumgehung“.*

Maßnahmen für Beschäftigte:

- Treten Sie in sozialen Netzwerken und Karriereplattformen möglichst datensparsam auf und vermeiden Sie Angaben zu konkreten Standorten, Aufgaben und Projekten. Seien Sie sich bewusst, dass solche Informationen in Verbindung mit anderen frei verfügbaren Daten zur Planung von Angriffen auf Sie oder ihr Unternehmen genutzt werden können.
- Trennen Sie private und dienstliche IT und greifen Sie auf Unternehmenssysteme nur mit aktivem VPN zu. Seien Sie vorsichtig bei der Nutzung Ihres Heimnetzwerks, insbesondere wenn es kein sicheres Schutzniveau bietet.
- Nutzen Sie für dienstliche Kommunikation möglichst nur die vorgesehenen unternehmenseigenen Geräte und abgesicherten Kommunikationskanäle. Verzichten Sie insbesondere auf private Messenger-Dienste oder ungesicherte Cloud-Dienste für betriebskritische Informationen.
- Achten Sie auf Anzeichen physischer Sabotage, etwa Beschädigungen an Umzäunungen, Drohnenüberflüge oder sonstige Ausspähversuche. Melden Sie entsprechende Beobachtungen – auch wenn diese zunächst banal erscheinen – konsequent und präzise über die dafür vorgesehenen Meldewege.
- Seien Sie sich bewusst, dass Sie durch Ihre Funktion besonders exponiert sein und deshalb in den Fokus ausländischer Nachrichtendienste geraten können. Öffentliche Meinungsäußerungen, gerade in sozialen Medien, können gegen Sie instrumentalisiert werden, um nachrichtendienstliche Ausforschungs- und Sabotageinteressen durchzusetzen. Dies kann auch ohne Ihr Wissen und von Ihnen unbemerkt geschehen.

  Mehr dazu in unseren Informationsblättern zum Wirtschaftsschutz zu „Social Engineering“.*

Maßnahmen zur sicheren Durchführung von Geschäftsreisen:

- Vermeiden Sie Reisen in SmbS. Beachten Sie bei unverzichtbaren Reisen die Reise- und Sicherheitshinweise des Auswärtigen Amtes und halten Sie sich über die aktuelle Lage auf dem Laufenden.
- Tragen Sie sich in die Krisenvorsorgeliste ELEFAND ein. Reisen Sie möglichst in Begleitung.
- Seien Sie skeptisch bei der Kontaktaufnahme durch Ihnen unbekannte Personen, um kompromittierende Situationen zu vermeiden.
- Vermeiden Sie jedes Verhalten, aus dem Spionagevorwürfe konstruiert werden könnten (z. B. Bild- oder Tonaufnahmen).
- Planen Sie Transportmittel und -routen vorab. Halten Sie sich von potentiell sensiblen Orten (z. B. Militäreinrichtungen) und gefährlichen Situationen (z. B. Protesten) fern.

  Mehr dazu in unseren Informationsblättern zum Wirtschaftsschutz zu „Sicherheit auf Geschäftsreisen“.*

Die wichtigsten Informationen und konkreten Handlungsempfehlungen zu den Phishing-Angriffen über Messengerdienste finden Sie auf der Website, die das BfV mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eingerichtet hat:

https://www.bsi.bund.de/dok/phishing-messengerdienste

https://www.bsi.bund.de/dok/phishing-signal-support

* Die Informationsblätter zum Wirtschaftsschutz finden Sie online bei den Produkten des Bereichs Prävention/Wirtschafts- und Wissenschaftsschutz unter:
https://www.verfassungsschutz.de/DE/themen/praevention_wirtschafts-wissenschaftsschutz/unsere-produkte/unsere-produkte_artikel.html

So erreichen Sie uns

Für Informationen zu Bedrohungen für Ihre Branche durch Spionage und Sabotage, Terrorismus oder gewaltbereiten Extremismus sowie für konkrete Sicherheitsanfragen oder Verdachtsfälle kontaktieren Sie den Bereich Wirtschaftsschutz:

wirtschaftsschutz@bfv.bund.de
+49 30 18792-3322

Natürlich steht Ihnen auch die Landesbehörde für Verfassungsschutz in Ihrem Bundesland als Ansprechpartner zur Verfügung. Sollte Ihnen der Kontakt nicht bekannt sein, vermitteln wir Ihnen diesen gerne.

Ihre Angaben werden in jedem Fall vertraulich behandelt.

PRÄVENTION
WIRTSCHAFTSSCHUTZ