Bundesministerium
des Innern

06. März 2026

Nationale Wirtschaftsschutzstrategie

Inhaltsverzeichnis

Zusammenfassung

Aufbauend auf nationalen und internationalen Zielsetzungen und des Ansatzes integrierter Sicherheit ebnet die Nationale Wirtschaftsschutzstrategie den Weg in den integrierten und ganzheitlichen Wirtschaftsschutz. Das heißt, alle betroffenen Bereiche der Politik, der Behörden und der Wirtschaft arbeiten eng zusammen, um im Sinne eines All-Gefahren-Ansatzes die Resilienz der deutschen Wirtschaft zu steigern. Deshalb gilt: Der Schutz der deutschen Wirtschaft kann nur so gut sein, wie es den staatlichen und privatwirtschaftlichen Akteuren gelingt, in einer gemeinsamen Ausrichtung und in sich ergänzender Weise zusammenzuarbeiten. Deshalb wollen wir den bestehenden offenen Dialog dazu mit der Wirtschaft, Verbänden und Unternehmen (eingeschlossen KMU) fortsetzen und vertiefen, unter Einbeziehung von wissenschaftlicher Expertise und in Abstimmung mit anderen Initiativen und Strategien wie der geplanten nationalen Wirtschaftssicherheitsstrategie.

Ausgangspunkt sind die im Februar 2024 vorgestellten Eckpunkte der Nationalen Wirtschaftsschutzstrategie. Dabei standen dort vor allem der integrierte Ansatz, die ressortübergreifende Koordinierung und die Weiterentwicklung der Initiative Wirtschaftsschutz[1] im Vordergrund. Die jetzt vorliegende Nationale Wirtschaftsschutzstrategie geht noch einen Schritt weiter: Zunächst wird zum ersten Mal eine Definition des staatlich organisierten Wirtschaftsschutzes vorgestellt, welche auch das übergeordnete Ziel des Wirtschaftsschutzes umfasst und diesen in den übergreifenden Kontext der Wirtschaftssicherheit einbettet: **Die Stärkung der Resilienz der Wertschöpfungs- und Lieferketten sowie von Forschung, Innovation und Entwicklung deutscher Unternehmen gegenüber sicherheitsbezogenen Herausforderungen und Bedrohungen (physisch, digital, hybrid).** Daraus werden drei Kernziele entwickelt:

- Weiterentwicklung der Rahmenbedingungen für Unternehmen und des Leistungsportfolios der Sicherheitsbehörden
- kollektive Resilienzsteigerung
- individuelle Resilienzsteigerung

Im nächsten Schritt werden passende Angebote und Maßnahmen vorgestellt, die zur Erreichung dieser Ziele beitragen und durch die Bundesregierung und ihre Partner umgesetzt werden. Eine besondere Stellung kommt hier der Initiative Wirtschaftsschutz zu, welche die Steuerung und das Monitoring der Umsetzung übernehmen wird.

Die Maßnahmen kommen dabei auch anderen gefährdeten gesellschaftlichen Gruppen z.B. im Bereich Wissenschaft oder Nichtregierungsorganisationen zu Gute.

---

[1] Die durch das BMI koordinierte Dachinitiative analysiert gemeinsam mit Expertinnen und Experten der Sicherheitsbehörden vom Bundesamt für Verfassungsschutz (BfV), Bundeskriminalamt (BKA), Bundesnachrichtendienst (BND) und Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundeskanzleramt (BKAmt) als vorgesetzte Behörde des BND, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), sowie den Spitzenwirtschafts- und Sicherheitsverbänden Bundesverband der deutschen Industrie (BDI), Deutsche Industrie- und Handelskammer (DIHK), Verband für Sicherheit in der Wirtschaft, Bundesverband (VSW) und Bundesverband der Sicherheitswirtschaft (BDSW) die Risikolage, entwickelt entsprechende Aktionspläne und setzt diese um.

1 Ausgangslage

Deutschlands Widerstands- und Wettbewerbsfähigkeit beruhen auf seiner hohen Innovationskraft und auf technologischer und digitaler Souveränität.[2] Ziel der nachfolgend aufgeführten Strategien und Initiativen ist es deshalb auch, die Widerstandsfähigkeit deutscher Unternehmen insgesamt zu stärken.

Im Mai 2023 haben die G7-Staaten eine gemeinsame Erklärung zu wirtschaftlicher Resilienz und Wirtschaftssicherheit veröffentlicht, welche u.a. auf resiliente Lieferketten und Kritische Infrastrukturen abzielt. Darin haben die G7-Staaten sich unter anderem darauf verständigt, den strategischen Dialog gegen böswillige Praktiken zu vertiefen, um globale Lieferketten vor unrechtmäßiger Einflussnahme, Spionage, unrechtmäßiger Weitergabe von Fachwissen und Sabotage im digitalen Raum zu schützen.

Mit der Nationalen Sicherheitsstrategie der Bundesregierung vom 14. Juni 2023 wurde die Weiterentwicklung der Nationalen Wirtschaftsschutzstrategie und der entsprechenden Aktionspläne bekräftigt.[3]

Mit ihrer Europäischen Strategie für Wirtschaftssicherheit[4] vom 20. Juni 2023 haben die Europäische Kommission und der Hohe Vertreter der Union für Außen- und Sicherheitspolitik ebenfalls den Schutz und die Stärkung der Resilienz der Wirtschaft in den Vordergrund gerückt. Ziele sind dabei die Stärkung der Resilienz von Wertschöpfungs- und Lieferketten und die Minderung von wirtschaftlichen Abhängigkeiten, der Schutz Kritischer Infrastrukturen, die Stärkung der technologischen Souveränität und der Technologiesicherheit sowie die Abwehr wirtschaftlichen Zwangs. Diese Ziele sollen durch eine Steigerung der Wettbewerbsfähigkeit (Promote), ein De-risking (Protect) und Zusammenarbeit mit Partnerländern (Partner) erreicht werden. Die Europäische Strategie für Wirtschaftssicherheit wird die Bundesregierung zudem mit einer Nationalen Wirtschaftssicherheitsstrategie flankieren, wie im Koalitionsvertrag angekündigt.

In der am 13. Juli 2023 veröffentlichten China-Strategie setzt die Bundesregierung auch einen Schwerpunkt auf den Schutz und die Stärkung der Resilienz der deutschen Wirtschaft angesichts der weiterhin gewollten engen wirtschaftlichen Verflechtung mit China. Im Vordergrund steht dabei das De-Risking durch die konsequente Reduktion strategischer Abhängigkeiten und die Diversifizierung von Lieferketten, die verbesserte Kontrolle von Investitionen, die Erhöhung der Forschungssicherheit und der Schutz von Schlüsseltechnologien und Kritischer Infrastruktur.

Die Einsetzung des Nationalen Sicherheitsrats ist ein weiterer wichtiger Meilenstein in der Sicherheitsarchitektur der Bundesrepublik Deutschland. Er koordiniert ressortübergreifend wesentliche Fragestellungen integrierter Sicherheitspolitik an den Schnittstellen innerer, äußerer, wirtschaftlicher und digitaler Sicherheit sowie ziviler und militärischer Verteidigung auf Ebene der Bundesregierung. Der Nationale Sicherheitsrat leistet Strategieentwicklung

---

[2] Nationale Sicherheitsstrategie, 2023, Seite 15

[3] Nationale Sicherheitsstrategie, 2023, Seite 56

[4] JOIN(2023) 20 final.

und strategische Vorausschau, u.a. durch eine Weiterentwicklung der Nationalen Sicherheitsstrategie.

Der Wirtschaftsschutz ist neben anderen Instrumenten der Wirtschaftssicherheit Gegenstand sicherheitspolitischer Erwägungen. Der Wirtschaftsschutz ist daher eine bedeutsame Komponente zur Erreichung des Ziels einer Stärkung der Resilienz von Wertschöpfungs- und Lieferketten im Rahmen der Wirtschaftssicherheit. Denn resiliente und dauerhaft leistungsfähige Unternehmen sind die Voraussetzung für die gesamtwirtschaftliche Stärke Deutschlands und zugleich ein wichtiger Pfeiler des gesellschaftlichen Zusammenhalts, des Wohlstands sowie der inneren und äußeren Sicherheit.

Im Kontext geopolitischer und geoökonomischer Herausforderungen nehmen Bedrohungen sowie deren Komplexität auch im Bereich der Wirtschaft weltweit zu. Die Hemmschwelle autoritärer Staaten für (Wirtschafts-) Spionage und Sabotage sinkt weiter. Hochprofessionelle kriminelle Akteure, auch aus den Strukturen der Organisierten Kriminalität, operieren teilweise im Auftrag und in enger Abstimmung mit staatlichen Sicherheitsorganisationen und Nachrichtendiensten. Die klare Unterscheidung zwischen staatlichen, nicht-staatlichen, sowie kriminellen und extremistischen bzw. terroristischen Gruppierungen verschwimmt zusehends. Hybride, digitale und analoge Bedrohungen verschmelzen zunehmend miteinander. Desinformationskampagnen, illegitime Einflussnahme, Spionageangriffe und Sabotage, Cyber-Angriffe, Erpressung und Diebstahl stören Wertschöpfungs- und Lieferketten von Unternehmen empfindlich oder unterbrechen sie gar. Deutsche Unternehmen werden gezielt von fremden Nachrichtendiensten und kriminellen Akteuren (zum Teil in staatlichem Auftrag) attackiert, Mitarbeitende gezielt angesprochen, um in den Besitz von Know-how und Innovationen zu gelangen.

Diesen Gefahren muss ein ganzheitlicher und integrierter Wirtschaftsschutz im engen Schulterschluss der staatlichen und privaten Akteure entgegentreten, um langfristig die Widerstandsfähigkeit der deutschen Wirtschaft zu stärken und die Wirtschaftssicherheit insgesamt zu erhöhen.

Daher hat die Bundesregierung Anfang 2024 Eckpunkte für die Nationale Wirtschaftsschutzstrategie und den Aktionsplan 2024+ vorgestellt. Darauf aufbauend wurde die hier vorgelegte Nationale Wirtschaftsschutzstrategie erarbeitet.

Hierzu hat die Bundesregierung verschiedene Interessengruppen eingebunden: Verbände, kleine und mittlere Unternehmen (KMU) sowie Großunternehmen hatten die Möglichkeit, ihre Ideen und Unterstützungsbedarfe in den Strategieprozess einzubringen. Darüber hinaus fand ein Erfahrungsaustausch mit verschiedenen internationalen Regierungen statt, dessen Ergebnisse ebenfalls in diese Strategie eingeflossen sind.

2 Wirtschaftsschutz in Deutschland

Bislang fehlte es an einer einheitlichen Definition zu dem Begriff Wirtschaftsschutz. Diese wird jedoch benötigt, um für alle Akteure ein gemeinsames Verständnis des Begriffs herzustellen und diesen auch in den Kontext von Wirtschaftssicherheit (im Englischen: economic security) zu stellen.

Definition

Staatlich organisierter Wirtschaftsschutz heißt:

Wirtschaftsschutz ist die staatlich unterstützte Stärkung der Fähigkeit deutscher Unternehmen, die Resilienz ihrer Wertschöpfungs- und Lieferketten sowie den Schutz von Forschungs-, Entwicklungs- und Innovationsaktivitäten gegenüber sicherheitsbezogenen physischen, digitalen und hybriden Bedrohungen wirksam zu erhöhen, insbesondere vor Wirtschaftsspionage und Wirtschaftssabotage.

Jenseits des Wirtschaftsschutzes ist hierfür bspw. auch die Reduzierung strategischer Abhängigkeiten von Drittstaaten durch die Diversifizierung von Lieferbeziehungen, europäische Produktion oder Vorratshaltung kritischer Güter sowie die Abwehr wirtschaftlichen Zwangs durch Drittstaaten zu nennen.

Hierzu hat der Nationale Sicherheitsrat bereits die Erarbeitung eines Aktionsplans zur Stärkung der strategischen Rohstoffversorgung beschlossen.

Verantwortlich für die Sicherheit ihres Unternehmens und ihrer dazugehöriger Lieferketten sind an erster Stelle die Unternehmen selbst. Die Bundesregierung und ihre nachgeordneten Behörden unterstützen diese durch ein zielgruppenspezifisches Leistungsportfolio, insbesondere durch die Gewinnung, Aufbereitung und Bereitstellung von Informationen. Hierzu gehören auch nachrichtendienstlich gewonnene Informationen (z.B. jährlicher Verfassungsschutzbericht des BfV, Sicherheitshinweise des BfV für die Wirtschaft). Außerdem schlagen die Sicherheitsbehörden bedrohungsabhängig geeignete Schutzmaßnahmen vor und klären allgemein zur Prävention auf. Zudem gestaltet die Bundesregierung die sicherheitspolitischen Rahmenbedingungen so, dass eine effektive Selbsthilfe für die Unternehmen umsetzbar ist. Im Kontext der Gesamtverteidigung und zur Stärkung der gesamtstaatlichen und gesamtgesellschaftlichen Resilienz unterstützt die Bundesregierung betroffene Unternehmen bei der Wahrnehmung ihrer spezifischen Absicherungs-, Schutz- und Verteidigungsverantwortung in Bedrohungslagen.

Eine besondere Stellung kommt hier den Verbänden zu, die die Interessen ihrer Mitgliedsunternehmen vertreten. Sie wirken auch als Multiplikatoren und Bindeglieder in die deutsche Wirtschaft und können so dazu beitragen, dass Unternehmen die Angebote der Bundesregierung erreichen. Hierbei gilt: Der Schutz der deutschen Wirtschaft kann nur so gut sein, wie es den staatlichen und privatwirtschaftlichen Akteuren gelingt, in einer gemeinsamen Ausrichtung und in sich ergänzender Weise zusammenzuarbeiten.

Ganzheitlicher und integrierter Wirtschaftsschutz

Wirtschaftsschutz im o.g. Sinne muss ganzheitlich im Real- und Cyber-Raum gedacht werden. Wirtschaftsschutz fokussiert sich hierbei im Sinne eines All-Gefahren-Ansatzes auf

physische, digitale und hybride Bedrohungen der globalen Wertschöpfungs- und Lieferketten sowie die Forschungs-, Entwicklungs- und Innovationsaktivitäten deutscher Unternehmen. Der Wirtschaftsschutz bettet sich ein in die Anstrengungen zur Erhöhung der Wirtschaftssicherheit und der nationalen Sicherheit insgesamt.

Wirtschaftsschutz muss außerdem integriert sein. Das heißt: Alle Bereiche der Politik, der Behörden und der Wirtschaft müssen eng zusammenarbeiten, um die Stärkung der Resilienz der Wertschöpfungs- und Lieferketten deutscher Unternehmen gemeinsam zu erreichen. Nur so kann integrierte Sicherheit für den Bereich des Wirtschaftsschutzes adaptiert werden und damit den kontinuierlichen Prozess des Zusammenwirkens staatlicher und privater Akteure stärken.

Ein ganzheitlicher und integrierter Wirtschaftsschutz erfordert von allen Beteiligten ein gemeinsames Verständnis für Ursache- und Wirkungsbeziehungen, von aktuellen und sich abzeichnenden Bedrohungen und Risiken, von Handlungsbedarfen sowie von Verantwortlichkeiten und Fähigkeiten.

Ressortübergreifende Koordination des Wirtschaftsschutzes

Für eine wirkungsvolle Unterstützung der physischen und digitalen Sicherheit von Unternehmen ist eine enge und vertrauensvolle Zusammenarbeit innerhalb der Bundesregierung notwendig. Im Sinne des integrierten Ansatzes müssen alle Bereiche der Politik dazu beitragen, die Resilienz der Wertschöpfungs- und Lieferketten deutscher Unternehmen und Wissenschaftseinrichtungen zu erhöhen.

Hierzu gehören auf Ebene der Ministerien neben dem Bundesministerium des Innern (BMI) als für Wirtschaftsschutz federführendes Ressort auch:

- das Bundeskanzleramt (BKAmt),
- das für Wirtschaftssicherheit federführende Bundesministerium für Wirtschaft und Energie (BMWE),
- das Bundesministerium der Verteidigung (BMVg),
- das Auswärtige Amt (AA),
- das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR),
- das Bundesministerium für Digitales und Staatsmodernisierung (BMDS),
- das Bundesministerium für Verkehr (BMV) und
- das Bundesministerium für Landwirtschaft, Ernährung und Heimat (BMLEH).

Hinzu kommen die nachgeordneten Behörden, hier insbesondere

- das Bundesamt für Verfassungsschutz (BfV),
- das Bundeskriminalamt (BKA),
- das Bundesamt für Sicherheit in der Informationstechnik (BSI),
- der Bundesnachrichtendienst (BND),
- das Bundesamt für den Militärischen Abschirmdienst (BAMAD) und
- das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

Darüber hinaus sind die Landesämter für Verfassungsschutz (LfV), die Landeskriminalämter (LKAs) und auch die lokalen Polizeidienststellen wichtige Ansprechpartner für die

Unternehmen vor Ort. Aufgrund der Vielzahl der staatlichen Akteure und Aktivitäten des Wirtschaftsschutzes sind eine zentrale Koordination und Moderation unerlässlich. Die Koordination des Wirtschaftsschutzes in der Bundesregierung obliegt – im Sinne der hier beschriebenen Ziele - ressortübergreifend dem für den Wirtschaftsschutz zuständigen Parlamentarischen Staatssekretär im Bundesministerium des Innern.

3 Der Weg zum ganzheitlichen und integrierten Wirtschaftsschutz

Ziel der Bundesregierung

Ziel der Bundesregierung ist die Stärkung der Resilienz deutscher Unternehmen und ihrer Wertschöpfungs- und Lieferketten sowie ihrer Forschung, Innovationen und Entwicklung gegenüber sicherheitsbezogenen Herausforderungen und Bedrohungen. Alle Maßnahmen im Bereich Wirtschaftsschutz sollen zu dieser Zielerreichung beitragen. Dazu stehen drei Kernziele im Vordergrund:

Kernziel 1: Die Rahmenbedingungen für die Unternehmen und die Leistungsportfolios der Sicherheitsbehörden weiterentwickeln

Ziel ist es, die rechtlichen Rahmenbedingungen für das Handeln der Unternehmen so zu gestalten, dass die Erhöhung der unternehmenseigenen Resilienz erreicht werden kann.

Zudem sollen die von den Sicherheitsbehörden erbrachten Unterstützungsleistungen („Hilfe zur Selbsthilfe“) bedarfsgerecht ergänzt und auf die aktuellen Bedarfe der Unternehmen – insbesondere der KMU – hin ausgerichtet werden.

Kernziel 2: Die kollektive Resilienz durch Zusammenarbeit der staatlichen und privaten Akteure verbessern

Ziel ist es, die kollektive Resilienz der Unternehmen und ihrer jeweiligen Wertschöpfungs- und Lieferketten zu stärken und hierbei die staatlichen Unterstützungsangebote gezielt einzusetzen.

Eine wesentliche Grundlage hierfür ist, dass sich das Zusammenwirken der privatwirtschaftlichen Akteure untereinander weiterentwickelt und ihre Zusammenarbeit und der Informationsaustausch mit den staatlichen Akteuren auf allen Ebenen verstärkt und auf die künftigen Herausforderungen ausgerichtet wird.

Kernziel 3: Die individuelle Resilienz in Wirtschaft und Wissenschaft stärken

Ziel ist es, die individuelle Resilienz aller innerhalb der jeweiligen Wertschöpfungs- und Lieferketten miteinander verbundenen Akteure zu stärken. Eine wesentliche Grundlage hierfür ist, dass die Unternehmen in der eigenen Organisation risikogerechte Mindeststandards für ihre Sicherheit in der physischen und in der digitalen Welt etablieren.

4 Handlungsfelder im Wirtschaftsschutz

Im Rahmen des Aktionsplans 2024+ aus den Eckpunkten der Nationalen Wirtschaftsschutzstrategie wurden bereits eine Vielzahl von Maßnahmen identifiziert, die hier den verschiedenen Kernzielen zugeordnet und um weitere Maßnahmen und Angebote erweitert werden.

Zu 1: Rahmenbedingungen für die Unternehmen und die Leistungsportfolios der Sicherheitsbehörden weiterentwickeln

Im Rahmen der Beteiligung von Verbänden, KMU und Großunternehmen waren die Rahmenbedingungen und das Leistungsportfolio der Sicherheitsbehörden ein wesentlicher Ansatzpunkt. Bei den (gesetzlichen) Rahmenbedingungen ging es den Stakeholdern insbesondere darum, dass diese einerseits die Sicherheit von Unternehmen wirksam unterstützen und den privaten Akteuren andererseits genügend Freiräume gelassen werden, um die Sicherheit innerhalb der Organisationen effizient und möglichst bürokratiearm zu gewährleisten.

Weiterentwicklung der relevanten Rahmenbedingungen

- Die Bundesregierung wird bei neuen Gesetzen oder Gesetzesänderungen Sicherheitsaspekte für die Wirtschaft und die Wissenschaft zukünftig stärker berücksichtigen. Beispielsweise sollte bei der Festlegung von gesetzlichen Veröffentlichungs- bzw. Berichtspflichten für Unternehmen unter Beachtung des Transparenzgebotes darauf geachtet werden, dass diese nicht zur Herausgabe solcher sensiblen Daten verpflichten, die für Spionage, Sabotage oder terroristische Anschläge genutzt werden können. Die Bundesregierung wird sich ebenfalls auf EU-Ebene für eine ausgewogene Position zwischen innovationsfördernden Datenzugängen und angemessenen Sicherheitsvorkehrungen zum Schutz sensibler Daten einsetzen.
- Mit der nationalen Umsetzung der Critical Entities Resilience Directive (EU-Richtlinie 2022/2257; CER-Richtlinie) wird erstmals ein übergreifender Rahmen für den physischen Schutz Kritischer Infrastrukturen in Deutschland etabliert. Ziel ist es, die Resilienz von Unternehmen der Kritischen Infrastruktur (KRITIS) zu erhöhen, die Funktionsfähigkeit der Wirtschaft und Infrastruktur zu stärken und im Ergebnis die Versorgung der Bevölkerung in Krisenfällen (z. B. Beeinträchtigung der Versorgung im Gesundheitswesen, bei Ernährung, in Transport und Verkehr sowie Wasser und Energie) sicherzustellen. In diesem Zuge werden die KRITIS-Unternehmen erstmalig durch bundeseinheitliche Vorgaben identifiziert, ein Verfahren für Risikobewertungen aufgesetzt, Mindestvorgaben für Resilienzmaßnahmen seitens der Betreiber festgelegt sowie ein Störungsmonitoring für die Betreiber etabliert.
- Die in der NATO erarbeiteten Leitlinien zu Resilienz (Baselinie Requirements) und Maßnahmen zu Wirtschaftsschutz wird die Bundesregierung umsetzen und gemeinsam mit NATO-Alliierten weiterentwickeln.
- Mit der Umsetzung der Network and Information System Security Directive 2 (NIS-2-Richtlinie) zielt die Bundesregierung auf die Einführung verbindlicher Maßnahmen für Verwaltung und Wirtschaft, mit denen in der gesamten Europäischen Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt wird. Wichtige und besonders wichtige

Einrichtungen werden vor Schäden durch Cyberangriffe geschützt und das Funktionieren des europäischen Binnenmarktes verbessert.
- Die Sicherheitswirtschaft (einschließlich Cybersicherheitswirtschaft) als Dienstleister für die Unternehmenssicherheit unterstützt Unternehmen bei der Bedarfsanalyse, Konzeption, Planung, Umsetzung und im Betrieb. Sie unterstützt insbesondere Unternehmen ohne eigene Sicherheitsabteilung. Ihr kommt daher eine besondere Aufgabe als Brücke des Wirtschaftsschutzes zu deutschen KMU zu und ist daher durch BDI, DIHK, BDSW und VSW in der Initiative Wirtschaftsschutz vertreten.
- Um die Sicherheit in Unternehmen zu erhöhen, wird das BMI den im Rahmen der Befragung von Großunternehmen vorgebrachten Wunsch prüfen, wie Regelungen zur Einführung von Verantwortlichen für Unternehmenssicherheit oder Wirtschaftsschutz möglichst bürokratiearm umgesetzt werden können. Dies sollte jedoch nicht unterhalb einer noch zu erörternden Unternehmensgröße erfolgen und das unbedingte Ziel verfolgen, die Unternehmenssicherheit zu steigern, sofern es keine vergleichbaren, ebenso wirksamen, aber weniger invasiven Mittel gibt.
- Für besonders sensible Bereiche in den Unternehmen ist es wichtig, vertrauenswürdiges Personal einzusetzen, um die Gefahr von Wissensabfluss oder Sabotage zu verringern. Das BMI prüft, welche Möglichkeiten für eine datenschutzkonforme Integritätsprüfung von Bewerberinnen und Bewerbern und Beschäftigten (Pre-Employment-Screening, Backgroundchecks) ggf. ohne Mitwirkung von Behörden geschaffen werden können.

Eine weitere Dimension dieses Kernzieles ist es, die bestehenden Leistungsportfolios der Sicherheitsbehörden im Bereich Wirtschaftsschutz zu evaluieren und weiter an den Bedürfnissen der Zielgruppen auszurichten.

Die Leistungsportfolios der Sicherheitsbehörden weiterentwickeln

- Die bisherigen Regelungen zur Ausgestaltung von jeweiligen Single Points of Contact (SPOC) in den Sicherheitsbehörden hat sich bewährt. Das BMI prüft, ob eine deutschlandweite Ansprech- und Verteilstelle bei einer Behörde für alle Themen des Wirtschaftsschutzes einzurichten ist und wie die Erreichbarkeiten erhöht sowie Wartezeiten verkürzt werden können.
- KMU als Innovationstreiber, „Hidden Champions“ und wichtige Teile der Lieferketten von KRITIS-Unternehmen haben häufig keine eigene Sicherheitsorganisation oder Ansprechpartner und daher meist keinen direkten Kontakt zu Sicherheitsbehörden und deren Leistungen. Daher weiten die Sicherheitsbehörden ihre Angebote – insbesondere zur Ansprache von gefährdeten KMU – in allen Bereichen aus. Hierzu werden auch neue Formate wie die Ansprache über Social-Media-Kanäle genutzt. Das BfV hat hierzu mit der stärkeren Nutzung ihres X-Kanals für Wirtschaftsschutzthemen einen ersten Schritt unternommen. Die Erweiterung auf andere soziale Netzwerke wird durch das BfV geprüft.
- Das BfV bietet eine Vielzahl von Produkten und Angeboten zur Prävention an, die auf der Website des BfV einem breiten Publikum zur Verfügung stehen. Die Bekanntheit dieses Angebots bei Bedarfsträgern wollen wir weiter steigern. Zudem werden zielgruppenspezifische Produkte an relevante Bedarfsträger verteilt. Hierzu gehören u.a. die Informationsblätter für Wirtschaftsschutz, aktuelle Sicherheitshinweise und das SPOC-Magazin sowie branchenspezifische Gesprächskreise. Um dieses Angebot weiter auszubauen, ist dauerhaft zu prüfen und zu bewerten, welche Informationen kritisch für den Schutz von Unternehmen sind. Diese sind schnell und unbürokratisch zur Verfügung zu stellen.

- Für den Themenbereich Cybersicherheit bietet das BSI eine Vielzahl von Produkten für unterschiedliche Zielgruppen (inklusive KMU) an und baut vor dem Hintergrund der Umsetzung der NIS-2-Richtlinie in deutsches Recht mit dem BSI-Portal und dem BSI Information Sharing Portal (BISP)[5] sein Angebot für die Wirtschaft derzeit erheblich aus. Dieses neue Angebot wollen wir den Bedarfsträgern bekannt machen. In herausgehobenen Fällen unterstützt das BSI Unternehmen darüber hinaus auch unmittelbar mit eigenem Personal bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme.
- Das BfV, der BND, das BSI, das BKA und das BBK führen mit Unterstützung der Verbände der Initiative Wirtschaftsschutz regelmäßige Sicherheitsbriefings für interessierte Unternehmen durch. In einem breiten Ansatz werden hier – soweit möglich - regelmäßig aktuelle Informationen zur Bedrohungslage aus den verschiedenen Zuständigkeiten an interessierte Unternehmen weitergegeben.
- Die Initiative Wirtschaftsschutz analysiert und bewertet kontinuierlich neue Technologien hinsichtlich Wertstiftung für den Wirtschaftsschutz einerseits sowie bezüglich Bedrohungen und Risiken für Wertschöpfungs- und Lieferketten andererseits. Diese Bewertungen bezieht die Initiative in ihre Maßnahmen ein. Hierzu greift sie auch auf wissenschaftliche Expertise und die Erkenntnisse der Wirtschaft zurück und bezieht internationale/multilaterale Austauschformate und Experten in die Umsetzung ein.

Zu 2: Die kollektive Resilienz durch Zusammenarbeit der staatlichen und privaten Akteure verbessern

Die Zusammenarbeit zwischen staatlichen und privaten Akteuren soll ausgebaut und verbessert werden. Hierzu gehört auch, neue Modelle der Zusammenarbeit zu entwickeln. Dabei ist zu beachten, dass der Informationsfluss in beide Richtungen erfolgen muss. Die privaten Akteure profitieren von Informationen und Lagebildern der Sicherheitsbehörden, während die Sicherheitsbehörden die Informationen der privaten Akteure nutzen, um ihre Lagebilder anzureichern und zu vervollständigen. Auch der Austausch zwischen privaten Akteuren untereinander soll durch neue Formate, etwa durch „best-practice“ Foren, angeregt werden, sodass diese noch besser voneinander lernen können.

Es wurden verschiedene Maßnahmen identifiziert, die dazu beitragen, die Interaktion weiter zu stärken, die Initiative Wirtschaftsschutz weiterzuentwickeln, die Reichweite des Wirtschaftsschutzes zu erhöhen und den internationalen Austausch zu verbessern.

Weiterentwicklung der „Initiative Wirtschaftsschutz“

Das BMI entwickelt die Initiative Wirtschaftsschutz weiter. Im Rahmen dieser Dachinitiative arbeiten die Sicherheitsbehörden und verschiedene Verbände gemeinsam daran, die in dieser Strategie festgelegten Ziele zu erreichen und die verschiedenen Maßnahmen gemeinsam mit der Bundesregierung umzusetzen. Dazu wird ein Steuerungs- und Arbeitsmodell eingesetzt, das den aktuellen Herausforderungen entspricht. Dieses Modell umfasst zwei Ebenen:

1 – Der Koordinierungskreis gibt die inhaltliche Richtung für die Arbeit der Initiative Wirtschaftsschutz vor. Dies beinhaltet insbesondere die Priorisierung der Aufgaben, die Billigung von Aktionsplänen, das Monitoring der Umsetzung der Maßnahmen aus den

[5] https://portal.bsi.bund.de/ zuletzt aufgerufen am 06.03.2026

Aktionsplänen und der Nationalen Wirtschaftsschutzstrategie sowie das Erteilen entsprechender Aufträge an aus seiner Sicht geeignete Partner der Initiative.

2 – Der Management-Kreis ist das Arbeitsgremium der Initiative Wirtschaftsschutz. Er nimmt Aufträge des Koordinierungskreises entgegen, koordiniert und bearbeitet sie. Der Management-Kreis kann zur Erfüllung der Aufträge, insbesondere zur Umsetzung der Maßnahmen aus den Aktionsplänen, temporäre Arbeitsgruppen mit konkreten Arbeitsauftrag bilden. Zu den Arbeitsgruppen können weitere Unternehmen und Experten, unabhängig von deren institutionellen Zugehörigkeit hinzugezogen werden.

Den Verbänden kommt hier insbesondere die Aufgabe zu, die zur Verfügung stehenden Informationen als Multiplikator an ihre Mitglieder weiterzugeben und diese an der Umsetzung der Maßnahmen zu beteiligen. Dabei verzahnt das BMI die Initiative Wirtschaftsschutz mit bereits bestehenden staatlichen Initiativen ähnlicher Zielsetzung, bspw. mit der Allianz für Cyber-Sicherheit. Aktuellen Entwicklungen im Bereich Wirtschaftsschutz steht die Initiative Wirtschaftsschutz offen gegenüber. Bei Bedarf wird sich die Initiative durch neue Mitglieder, die Hinzuziehung von Experten und neuer Strukturen anpassen. Dazu könnte bspw. der gestiegene Bedarf an verstärkter Zusammenarbeit im Kontext Gesamtverteidigung gehören.

Zusammenarbeit staatlicher und privatwirtschaftlicher Akteure verbessern:

- Die Bundesregierung strebt an, die bestehenden Gesprächsformate zwischen Wirtschaft und Staat zu Sicherheitsthemen in ein Netzwerk zu integrieren, welches Unternehmen aller Größen und Branchen die Möglichkeit gibt, in den Austausch mit den relevanten staatlichen Akteuren zu kommen. Hierzu werden bestehende Austauschformate und Gesprächsrunden im Bereich des Wirtschaftsschutzes analysiert, auf Redundanzen geprüft und – sofern erforderlich – konsolidiert. Dies betrifft zum Beispiel die Unabhängige Partnerschaft Kritischer Infrastrukturen (UP-KRITIS), die Allianz für Cybersicherheit sowie die DAX 40 Runde des BSI, die Global Player Initiative und die Netzwerktreffen Wirtschaftskriminalität des BKA, Branchenspezifische Gesprächskreise des BfV sowie das gemeinsame Sicherheitsbriefing aller Sicherheitsbehörden.
- Am Ende soll hier ein Format entstehen, das, angelehnt an den Domestic Security Alliance Council (DSAC) der US-Regierung, viele der bestehenden Gesprächsformate zusammenfasst und so den Austausch für alle Akteure transparenter und einfacher macht. Erfolgreich bestehende Gesprächsformate sollen beibehalten werden.
- In diesem Rahmen sollen u.a. Formate zum Austausch zwischen staatlichen und privaten Akteuren zur strategischen Früherkennung und Szenarienbildung im Kontext Wirtschaftsschutz entwickelt werden. In Workshops sollen mögliche Szenarien erkannt und gemeinsame Lösungsansätze diskutiert werden. Hiervon sollen beide Seiten profitieren, damit drohende Gefahren erkannt, mögliche Handlungsoptionen abgeleitet und ein besseres Verständnis für die jeweiligen Perspektiven erarbeitet werden können. Bei größeren Bedrohungslagen könnte so auf das aufgebaute Wissen zurückgegriffen und die Lage besser bewältigt werden. Darauf aufbauend wird die Bundesregierung Informationsketten für Sicherheitshinweise, die Alarmierungswege für den Fall von konkreten Gefährdungen sowie die Reaktions- und Interaktionsfähigkeit staatlicher und privater Akteure analysieren und mit den entsprechenden Akteuren optimieren, um die schnelle und zielgerichtete Verteilung von Informationen im Ernstfall sicherzustellen.

- Die Partner der Initiative Wirtschaftsschutz moderieren „best practice“-Austausche zum Wirtschaftsschutz insbesondere für Start-ups und KMU, um einen einfacheren Einstieg in Sicherheitsthemen zu bieten. Hierzu werden erfolgreiche Praxisbeispiele gesammelt und wo möglich in einem „peer-to-peer“ Verfahren an Unternehmen mit ähnlichen Rahmenbedingungen weitergegeben.
- Um den Austausch zwischen Wirtschaft und Behörden zu stärken, ist es wichtig, dass es Personal gibt, das beide Seiten gut kennt und als Bindeglied fungieren kann. Ziel ist es, eine höhere Durchlässigkeit in beide Richtungen zu erreichen. Die Bundesregierung wird den Austausch von Personal im Rahmen von wechselseitigen Hospitationen und entsprechenden Formulierungen bei Stellenausschreibungen einzelfallabhängig prüfen und ggf. unterstützen.

Reichweite des Wirtschaftsschutzes erhöhen:

- Die Erfahrungen im Wirtschaftsschutz zeigen, dass bislang fast nur solche Unternehmen durch den staatlich organisierten Wirtschaftsschutz erreicht werden, die eine verantwortliche Person für Sicherheit haben. Bei einem sehr großen Teil der deutschen Wirtschaft ist eine solche Stelle nicht eingerichtet.
- Daher wird die Initiative Wirtschaftsschutz insbesondere in Abstimmung mit Landesbehörden, den IHKs und weiteren Branchenverbänden neue Konzepte für die Anbindung kleiner und mittlerer Unternehmen an den staatlich organisierten Wirtschaftsschutz erarbeiten. In Rahmen dieser Maßnahmen soll auch die Identifikation und Einbindung zusätzlicher, relevanter Akteure wie z.B. Universitäten mit einschlägigen Forschungsdisziplinen in den nationalen Wirtschaftsschutz gelingen. Dies ist insbesondere in Hinblick auf den Schutz von Forschung und Innovationen von hoher Bedeutung.
- Es ist von entscheidender Bedeutung, die Bedarfe der Zielgruppen zu kennen, um die passenden Angebote zur Verfügung zu stellen. Das BMI hat daher den benötigten Unterstützungsbedarf von Start-ups, KMU und Großunternehmen ermittelt und die angesprochenen Bedarfe in die hier vorliegende Strategie einfließen lassen. Dabei zeigten sich deutliche Überschneidungen zwischen den Bedarfen von KMU und Großunternehmen. Die Bedarfsermittlung wird in einem regelmäßigen, strukturierten Prozess wiederholt. Das Produktportfolio der Sicherheitsbehörden und die Aktionspläne Wirtschaftsschutz werden laufend an die Ergebnisse angepasst.
- Die im Aktionsplan 2024+ genannte Plattform für den Austausch von staatlichen und privaten Akteuren zu Bedrohungen und Risiken für Wertschöpfungs- und Lieferketten unter Berücksichtigung von bereits etablierten Initiativen soll als Erweiterung des Information Sharing Portal des BSI umgesetzt werden. Ziel ist es, Informationen zu Bedrohungen und Risiken zusammenzuführen, zu konsolidieren und bedarfsgerecht zur Verfügung zu stellen. Dadurch wird die Früherkennung von Bedrohungen und Risiken verbessert.
- Das BMI plant ein Modellprojekt der aufsuchenden Information und Beratung in sozialen Medien. Damit sollen die herkömmlichen Wege, wie Zusammenarbeit mit Verbänden, Nutzung bestehender Medien (Websites, Broschüren etc.) mit neuen, digitalen Zugangswegen mittels sozialer Medien (z. B. Xing, LinkedIn u. a.), KI-Chatbots oder (Online-)Veranstaltungen erprobt, analysiert und kombiniert werden. Ziel ist es, auch solche Unternehmen zu erreichen, die noch keine Berührungspunkte mit Sicherheitsthemen haben und sie für Wirtschaftsschutz zu sensibilisieren und in ihren Kompetenzen zu stärken.

Lagebild zum Nationalen Wirtschaftsschutz

- Die Bundesregierung strebt den Aufbau eines ganzheitlichen Lagebildes für den Wirtschaftsschutz an. Es soll anhand von Kennzahlen einen Überblick über die Ist-Situation und die Entwicklung im nationalen Wirtschaftsschutz ermöglichen.
- Das Lagebild beinhaltet ein Management-Cockpit, das steuerungsrelevante Informationen für die Koordinierung des Wirtschaftsschutzes enthält. Auch das Monitoring der Strategieumsetzung, das Erkennen von Nachsteuerungsbedarfen und das Messen der Zielerreichung soll ermöglicht werden. Das BMI wird mit Partnern die von den Sicherheitsbehörden zur Verfügung gestellten Daten sammeln, aufbereiten und der Wirtschaft die (nicht geheimhaltungsbedürftigen) Informationen zur Verfügung stellen. Das Lagebild soll die Unternehmen in der Bedeutung von Investitionen in ihre eigene Resilienz sensibilisieren.
- Als erster Schritt in diese Richtung werden methodisch einheitliche Standards erarbeitet Insbesondere geht es darum, Definitionen zu harmonisieren sowie Risiken innerhalb der Sicherheitsbehörden zu skalieren.

Internationaler Austausch:

- Die Bundesregierung wird prüfen, ob und wie ein internationales Netzwerk der Bundesrepublik Deutschland im Ausland als Anlaufstelle für die internationalen Vertretungen deutscher Unternehmen in Fragen des Wirtschaftsschutzes – angelehnt an die US-Behörde Overseas Security Advisory Council (OSAC)[6] – aufgebaut wird. Dieses Netzwerk würde an den Auslandsvertretungen der Bundesrepublik Deutschland angesiedelt werden und die Auslandshandelskammern eng einbeziehen.
- Die Bundesregierung wird die behördliche Zusammenarbeit mit EU-Mitgliedstaaten und EU-Behörden sowie im Rahmen der NATO im Bereich des Wirtschaftsschutzes weiter ausbauen. Wo passend, werden BMWE, AA und BMI das Thema Wirtschaftsschutz auch in die bilateralen Wirtschaftssicherheitsdialoge einbringen.
- Die Bundesregierung prüft, ob durch das an den jeweiligen Auslandsvertretungen eingesetzte Personal ein „internationaler Regulatorik-Monitor“ etabliert werden kann, der sich abzeichnende Veränderungen der Regulatorik mit Auswirkungen auf die Unternehmenssicherheit in wichtigen Auslandsmärkten kontinuierlich verfolgt, bewertet und die Unternehmen frühzeitig über zu erwartende Auswirkungen („was das für Ihr Unternehmen bedeutet“) informiert.

Zu 3: Die individuelle Resilienz in Wirtschaft und Wissenschaft stärken

Ziel ist es, die individuelle Resilienz der Wirtschaft und der Wissenschaft gegenüber sicherheitsbezogenen Herausforderungen und Bedrohungen zu erhöhen.

Um insbesondere KMU sowie Forschungseinrichtungen dabei zu unterstützen, sich selbst vor Angriffen aus dem Realraum und dem Cyberraum besser zu schützen und die Widerstandskraft ihrer eigenen Organisation zu erhöhen, stellen die Bundesregierung und die nachgeordneten Behörden, teilweise in Zusammenarbeit mit den Ländern, verschiedene Leitlinien und Handlungsempfehlungen zur Verfügung und entwickeln diese kontinuierlich

[6] OSAC ist ein globales Netzwerk, das Vertretungen in verschiedensten Ländern unterhält und den dort tätigen US-Unternehmen Ansprechpartner bietet und vor aktuellen globalen und lokalen Risiken warnt.

weiter. Zudem ist geplant, die Qualifizierungsangebote im Bereich Wirtschaftsschutz und Unternehmenssicherheit auszubauen.

- Unternehmenssicherheit - DIN SPEC Corporate Security
  Unter Schirmherrschaft des BMI wird aktuell eine DIN-SPEC mit dem Titel „Corporate Security Anforderungen zur Stärkung physischer Resilienz von Organisationen“ erarbeitet. Ziel ist es, einen Standard für die physische Sicherheit von Unternehmen, Konzernen und anderen Organisationen zu erstellen. Im Rahmen der Erstellung dieser DIN SPEC ist angestrebt, verschiedene Sicherheitslevel bzw. Schutzniveaus zu definieren, die von den Organisationen in Abhängigkeit von der jeweiligen Asset-Kritikalität, ihrer wirtschaftlichen Leistungsfähigkeit und ihrer Risiko-Exposition angestrebt werden können - womit sich ein breites Spektrum von möglichen Nutzern (von KMU bis „Global Player“ oder auch andere Arten von Organisationen) eröffnen soll. Dies ermöglicht eine passgenaue Balance aus Aufwand und Sicherheitsbedarf. Aufbauend auf der DIN-SPEC wird angestrebt, zukünftig eine DIN-Norm zur Unternehmenssicherheit zu erstellen und diese auch auf die internationale Ebene zu erweitern. Dies unterstützt die Transparenz und Vergleichbarkeit von Sicherheitsvorkehrungen in verschiedenen Ländern und schafft Anreize, diese zu etablieren und zu stärken.

- Forschungssicherheit – BMFTR
  Forschungssicherheit ist die Antizipation und das Management von Risiken wie dem unerwünschten Wissens- und Technologieabfluss, insb. bei Zukunftstechnologien, der unzulässigen Einflussnahme und der missbräuchlichen Zweckentfremdung von Forschungsergebnissen. Dies schließt den Schutz vor Cyberspionage und -sabotage sowie das Risiko ungewollter Datenabflüsse über vernetzte Komponenten oder KI-Systeme aus Drittstaaten ein. Darüber hinaus ist der Schutz vor Wissens- und Technologieabfluss über die Abwerbung, Spionage oder das Aushorchen von Wissensträgern umfasst. Forschungssicherheit dient neben dem Schutz wissenschaftlicher Akteure auch der Wahrung langfristiger Wettbewerbsfähigkeit und nationaler Sicherheit. Sie ist entscheidend dafür, dass deutsche Innovationen auch dem deutschen Wohlstand zugutekommen und hat im Hinblick auf die geopolitische Bedrohungslage und zunehmende systemische Rivalitäten hohe Priorität. Hierbei ist nicht nur staatlich geförderte Forschung, sondern auch die Forschungszusammenarbeit zwischen deutschen Unternehmen und Unternehmen und Institutionen in Drittstaaten im Fokus. Das BMFTR initiierte daher im Herbst 2024 einen Stakeholderprozess, um gemeinsam mit Beteiligten aus Bundesregierung, Ländern und der Allianz der Wissenschaftsorganisationen einen ganzheitlichen Ansatz zur Stärkung der Forschungssicherheit zu erarbeiten. Im Dezember 2025 erfolgte eine Verständigung auf Eckpunkte zur Stärkung der Forschungssicherheit und zum Aufbau einer Nationalen Plattform für Forschungssicherheit[7], die ab 2026 umgesetzt werden sollen.

- Cybersicherheit - Grundschutz++
  Der Grundschutz++ liefert ein fachliches Fundament und ein umfangreiches Arbeitswerkzeug zur Implementierung und Weiterentwicklung eines Managementsystems

[7] Eckpunkte zur Stärkung der Forschungssicherheit und zum Aufbau einer Nationalen Plattform für Forschungssicherheit: https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2025/25-eckpunkte-forschungssicherheit.pdf?__blob=publicationFile&v=1 zuletzt aufgerufen am 06.03.2026

für Informationssicherheit in Institutionen. Der Grundschutz++ ist Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Institutionen (Behörden, Unternehmen etc.), die sich mit der Absicherung ihrer Geschäfts- und Verwaltungsprozesse sowie der zugehörigen Informationen, Anwendungen, IT-Systeme, Netze etc. befassen wollen. Dabei ist ein ganzheitlicher Ansatz zur Informationssicherheit zentral: Grundschutz++ betrachtet technische, infrastrukturelle, organisatorische und personelle Aspekte.
Der Grundschutz++ ist prozessorientiert angelegt und legt mit den maschinenlesbaren Anforderungen einen Grundstein für die Automatisierung. Perspektivisch soll der Grundschutz++ nicht nur flexibel anwendbar, sondern auch messbar sein. Seine wesentlichen Bestandteile sind die Methodik, die Anforderungen, eine Risikoanalyse und perspektivisch auch Kennzahlen. Der Anwenderkatalog Grundschutz++ enthält unter anderem atomare Sicherheitsanforderungen in verschiedenen Formaten, die in der „Stand der Technik-Bibliothek“ zur Verfügung stehen. Diese Plattform wird alle Anforderungen und Maßnahmen zentral bereitstellen. Auf Basis der Methodik-Grundschutz++ und der Anwenderkataloge Grundschutz++ kann in einer Institution ein Managementsystem für Informationssicherheit (ISMS) implementiert werden.
Der Grundschutz++ richtet sich an ein breites Spektrum von Institutionen und berücksichtigt deren unterschiedliche Ausgangslagen, Ressourcen und Bedürfnisse. Ergänzend dazu bietet der BSI-Standard 200-4 eine praxisnahe Anleitung, um ein Business Continuity Management System (BCMS) in der eigenen Institution zu etablieren. Der BSI-Standard 200-4 geht insbesondere auf die möglichen Synergiepotentiale mit den angrenzenden Themen der Informationssicherheit und des Krisenmanagements ein und stellt somit einen zentralen Bestandteil zur organisatorischen Resilienz dar.

- Cybersicherheit – CyberRisikoCheck nach DIN SPEC 27076 – IT-Sicherheitsberatung für kleine und Kleinstunternehmen
  Beim CyberRisikoCheck befragt ein IT-Dienstleister ein Unternehmen in einem ein- bis zweistündigen Interview zur IT-Sicherheit im Unternehmen. Darin werden 27 Anforderungen aus sechs Themenbereichen daraufhin überprüft, ob das Unternehmen sie erfüllt. Für die Antworten werden nach den Vorgaben der DIN SPEC Punkte vergeben. Als Ergebnis erhält das Unternehmen einen Bericht, der u. a. die Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält. Die Handlungsempfehlungen sind nach Dringlichkeit gegliedert und enthalten Hinweise darauf, welche staatlichen Fördermaßnahmen (auf Bundes-, Landes- und kommunaler Ebene) das jeweilige Unternehmen in Anspruch nehmen kann. Der CyberRiskoCheck ist keine IT-Sicherheitszertifizierung. Er ermöglicht einem Unternehmen jedoch bei geringem Aufwand eine Positionsbestimmung des eigenen IT-Sicherheitsniveaus und zeigt auf, welche konkreten Maßnahmen ein Unternehmen umsetzen bzw. bei einem IT-Dienstleister beauftragen sollte. Er richtet sich insbesondere an Unternehmen mit weniger als 50 Beschäftigten und soll Hürden zum Einstieg in mehr Cybersicherheit senken. Die DIN SPEC ist im Rahmen des *Projekts „mIT Standard sicher“* aus Mitteln des BMWE-Förderschwerpunkts Mittelstand-Digital (s.u.) entwickelt worden.

- Cybersicherheit – NKCS
  Das Nationale Koordinierungszentrum für Cybersicherheit (NKCS) informiert und berät Unternehmen, Start-Ups und Forschungseinrichtungen im Bereich Cybersicherheit zu den europäischen Förderprogrammen „Digital Europe“ und „Horizon Europe“. Das NKCS bildet das nationale Koordinierungszentrum des Europäischen Kompetenzzentrums für

Cybersicherheit in Industrie, Technologie und Forschung (ECCC). Zudem vertritt das NKCS nationale Interessen in europäischen Gremien und stärkt durch Workshops, Beratungen und Fachkonferenzen die nationale Cybersicherheitscommunity. Darüber hinaus baut es Strukturen auf, die die Cybersicherheitskapazitäten in Deutschland nachhaltig erhöhen. Das NKCS erhöht durch seine Tätigkeiten die Resilienz und Abwehrfähigkeit in Deutschland und der EU.

- Cybersicherheit - Förderschwerpunkt Mittelstand-Digital
  Der Förderschwerpunkt Mittelstand-Digital[8] des BMWE besteht aus dem bundesweiten Netzwerk der Mittelstand-Digital Zentren sowie der Initiative „IT-Sicherheit in der Wirtschaft“. Die Förderung der Mittelstand-Digital Zentren endet schrittweise bis Ende Dezember 2026. In dem neuen, ab 2027 aufzubauenden Netzwerk der Mittelstand-Digital Zentren sollen sog. CYBERsicher-Trainer KMU, Start-ups und Handwerk gezielt zu IT- und Cybersicherheitsfragen unterstützen.
  Im Zentrum der Initiative „IT-Sicherheit in der Wirtschaft“ steht die Transferstelle Cybersicherheit im Mittelstand[9] (Laufzeit bis 30.06.2027, optional Verlängerung um weitere zwei Jahre). Sie ist die zentrale Anlaufstelle für KMU sowie das Handwerk und adressiert explizit auch Start-ups. Sie übernimmt eine anbieterneutrale Lotsenfunktion, damit sich Unternehmen in der Angebotsvielfalt von Cybersicherheitslösungen zurechtfinden. Zudem arbeitet sie eng mit den Mittelstand-Digital Zentren zusammen. Die Transferstelle kümmert sich mit ihren kostenfreien Tools, Schulungen und Lernangeboten von der Prävention (CYBERsicher Check) über die Detektion bis hin zur Reaktion (CYBERsicher Notfallhilfe) um die Cybersicherheitsanliegen der Unternehmen.
  Zur Initiative IT-Sicherheit in der Wirtschaft gehören ebenfalls breitenwirksame Fokusprojekte, die sich spezifischen IT- und Cybersicherheitsherausforderungen von KMU widmen. Die Fokusprojekte erarbeiten z.B. Unterstützungsangebote zu Anforderungen aus neuen Rechtsakten (z.B. FitNIS2-Navigator[10], EasyCRA). Mit dem neuen Fokusprojekt ReACD[11] ist derzeit ein spielbasierter Lernansatz in Arbeit, mit dem die Handlungsfähigkeit von KMU-Mitarbeitenden bei Cybersicherheitsvorfällen und Datenverlust gesteigert werden soll. Ab August 2026 soll mit EvaSecur[12] eine kostenfreie Software sowie Schulungen für den Basisschutz Cybersicherheit von Prozessanlagen (z.B. Biogas-, Produktions- und Abfüllanlagen, Heizkraftwerke) in KMU verfügbar sein.

- Hybride Bedrohungen – Handreichung und Strategie
  Hybride Bedrohungen bezeichnen koordinierte, illegitime Vorgehensweisen eines Staates oder staatsnaher Organisationen zur Durchsetzung eigener Interessen zum Nachteil eines anderen Staates, die außerhalb des Rahmens eines konventionellen militärischen Angriffs bleiben. Die Bund-Länder offene Arbeitsgruppe Hybride Bedrohungen (BLoAG Hybrid) hat eine Handreichung zum Thema hybride Bedrohungen erstellt und veröffentlicht[13].

---

[8] https://www.mittelstand-digital.de/ zuletzt aufgerufen am 06.03.2026

[8] https://transferstelle-cybersicherheit.de/ zuletzt aufgerufen am 06.03.2026

[10] https://fitnis2.de zuletzt aufgerufen am 06.03.2026

[11] https://reacd.th-koeln.de/ zuletzt aufgerufen am 06.03.2026

[12] https://evasecur.de zuletzt aufgerufen am 06.03.2026

[13] https://www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html, zuletzt aufgerufen am 06.03.2026

Anhand von elf möglichen Maßnahmen wird aufgezeigt, wie der Schutz gegen hybride Bedrohungen verbessert werden kann. Aktuell wird die Strategie zu hybriden Bedrohungen durch die Bundesregierung erarbeitet, welche unter anderem Ansätze zum Schutz der Wirtschaft, Wissenschaft und Kritischer Infrastrukturen erfassen soll, da diese Bereiche häufig Ziel hybrider Bedrohungen sind. Der im November 2025 vom Nationalen Sicherheitsrat beschlossene Aktionsplan zur Abwehr hybrider Bedrohungen koordiniert die weitere ressortgemeinsame Arbeit in diesem Themenfeld.
Die Bundesregierung sieht in der Aus- und Weiterbildung im Wirtschaftsschutz und in der Unternehmenssicherheit eine wichtige Säule zur Erreichung der oben genannten Ziele. Eine kontinuierliche Aus- und Weiterbildung ist das Fundament für die Umsetzung von nachhaltigen und effektiven Schutzstrategien in Staat und Wirtschaft. Die Initiative Wirtschaftsschutz erarbeitet daher eine Übersicht zu den bestehenden Aus- und Weiterbildungsangeboten und stellt diese interessierten Akteuren zur Verfügung.

Impressum

Herausgeber

Bundesministerium des Innern, 11014 Berlin
Internet: www.bmi.bund.de

Stand
März 2026

Artikelnummer
BMI26004

Weitere Publikationen der Bundesregierung zum Herunterladen und zum Bestellen finden Sie unter:
www.publikationen-bundesregierung.de