
ASW
Bundesverband
Gemeinsam unsere Interessen schützen —
Wirtschaftsschutz und sichere Arbeitsplätze in Zeiten von Risiken und Veränderungen

Positionspapier des ASW Bundesverbandes „Wirtschaftsschutz 2025“

zur Bundestagswahl 2021 und für die 20. Legislaturperiode des Deutschen Bundestags

ASW
Bundesverband

Inhalt

Die Welt der Wirtschaft steht Kopf

Management Summary

Die Wirtschaft befindet sich mitten im Prozess der digitalen Transformation und der Industriestandort Deutschland ist mit seinen Unternehmen zunehmenden Risiken ausgesetzt. In den letzten Jahren wurden in Wirtschaft, Wissenschaft und von staatlicher Seite große Anstrengungen unternommen, die Cybersicherheit und den Wirtschaftsschutz von Produkten, Dienstleistungen wie auch in Unternehmen und Behörden zu verbessern. Die Bedrohungslage hat sich dennoch verschärft, denn Abwehrmaßnahmen und die Sicherheitsinformations-technologie haben nicht Schritt gehalten mit der Breite und Intensität von Cyberangriffen und Spionageaktivitäten.

Für Kriminelle, wie auch für fremde Nachrichtendienste sind Cyberangriffe über das Internet hochattraktiv, da eine Vielzahl von Schwachstellen in Soft- und Hardware-Produkten permanent neue Ansatzpunkte für die Entwicklung von Schadprogrammen liefern und durch die Möglichkeiten der Anonymisierung die Zurechenbarkeit und Ahndung von Angriffen erschwert wird.

Insbesondere Wirtschaftskriminalität und Wirtschafts- bzw. Industriespionage stellen eine reale Bedrohung für deutsche Unternehmen dar. Dabei sind drei Kategorien von Geschäftsgeheimnissen, die besonders schützenswert sind, hervorzuheben: Forschungsdaten, Produkt-spezifikationen und Fertigungstechnologien. Deren Attraktivität liegt meist in einem spezifischen Entwicklungsverfahren, einer herausragenden Qualität oder einer Fertigung mit sehr viel besserer Kosteneffizienz im Vergleich zu den Wettbewerbern. Die Wirtschafts-kriminalität hat sich weltweit zu einem hochprofitablen Modell entwickelt. Insbesondere das Internet spielt als Tatort eine große Rolle und wird als Mittel für die Begehung von Straftaten instrumentalisiert.

Der Extremismus stellt mit zunehmender Radikalisierung und Populismus in der Gesellschaft auch eine Gefahr für die deutsche Wirtschaft dar. Fünf Entwicklungen haben für unsere Unternehmen eine hohe Relevanz: gewaltsame Angriffe, Protestaktionen, Radikalisierung von Mitarbeitern, Reputations- und Kollateralschäden.

Zudem gewinnen externe Faktoren immer mehr an Bedeutung. Pandemien, Extremwetterereignisse und Naturkatastrophen werden zukünftig verstärkt auftreten und Auswirkungen auf den Standort Deutschland sowie die Welt haben.

Ausfall von Lieferketten und Mitarbeitenden, Betriebs-unterbrechungen sowie die Folgen von Unruhen und Protesten stellen ein hohes Risiko für alle Unternehmen dar.

Ziel muss es sein, einen strategischen, umfassenden und vernetzten Wirtschaftsschutz zu etablieren. Dieser muss über das IT-Sicherheitsgesetz hinausgehen und darf sich nicht allein auf IT-bezogene Maßnahmen fokussieren. Er umfasst auch organisatorische und personelle Schutzmaßnahmen. Hierbei nimmt der Faktor Mensch eine Schlüsselrolle ein. Ein enger und vertrauensvoller Erfahrungsaustausch zwischen staatlichen Stellen und Unternehmen ist Basis für einen erfolgreichen Wirtschaftsschutz. Aus Sicht des ASW Bundesverbandes besteht dringender Handlungsbedarf und ein klares Bekenntnis der Politik für den Wirtschaftsschutz!

Aus Sicht des ASW Bundesverbandes sind damit folgende Forderungen verbunden:

Forderungen

1. Einführung eines Koordinators für den Wirtschaftsschutz auf Bundesebene. Sicherheit ist das Fundament für Innovation, Durchsetzungskraft und Erfolg unserer Wirtschaft. Diese Sicherheit ist eine gemeinsame Verantwortung. Um diese wahrzunehmen, benötigen wir auf Bundesebene ein „Gesicht für den Wirtschaftsschutz".

2. Regelmäßiger Austausch auf höchster Ebene mit Treffen auf Staatssekretärs-Ebene bzw. mit dem Koordinator für den Wirtschaftsschutz sowie mit den Vorsitzenden der beteiligten Wirtschaftsschutzverbände im Rahmen des Steuerungskreises der Initiative Wirtschaftsschutz.

3. Transparenz über die aktuelle Gefährdungslage durch Einrichtung einer Nationalen Analyse- und Strategieplattform für Wirtschaftsschutz.

4. Verstärkung der regionalen Sicherheitspartnerschaften und Bündelung der Aktivitäten unter der „Initiative Wirtschaftsschutz".

5. Ausbau der internationalen Zusammenarbeit im Wirtschaftsschutz, um deutsche Unternehmen auf globalen Handelsrouten und internationalen Märkten zu schützen.

6. Stärkung der Geheimschutzbetreuung des Bundes für Wirtschaftsunternehmen sowie Beratung von Firmen in der Beschaffung und im Betrieb von Verschlusssachen (VS)-Technik durch staatliche Stellen.

7. Präzisierung der gesetzlichen Grundlagen, um deutsche Sicherheitsbehörden zu ermächtigen, Aktivitäten fremder Gruppierungen, die Wissenschaft und Wirtschaft schaden, aufzuklären.

8. Einrichtung eines anlassbezogenen Security Boards mit den sicherheitsbehördlichen und verbandsseitigen Partnern der Initiative Wirtschaftsschutz.

9. Weitere Unterstützung des deutschen Mittelstandes im Basisschutz durch Fortsetzung und Ausweitung des Projektes Wirtschaftsgrundschutz.

Einleitung

In den letzten Jahren wurden in der Wirtschaft, in der Wissenschaft und von staatlicher Seite große Anstrengungen unternommen, die Cybersicherheit und den Wirtschaftsschutz in Produkten, Dienstleistungen wie auch in Unternehmen und Behörden zu verbessern. Die Bedrohungslage hat sich dennoch verschärft, d.h. Abwehrmaßnahmen und die Sicherheitsinformationstechnologie haben nicht Schritt gehalten mit der Breite und Tiefe von Cyberangriffen und Spionageaktivitäten.

Unter dem Stichwort „assume the breaches" ist heute davon auszugehen, dass präventive Maßnahmen allein keinen hinreichenden Schutz bieten, sondern das moderne Schutzkonzepte auch eine effiziente Detektion und professionelle Reaktion beinhalten müssen, um die Wirkung von Angriffen zu minimieren. Deutsche Expertise ist weiterhin gefragt in einer vernetzten und sich stetig weiter entwickelnden Welt. Sowohl fremde Nachrichtendienste als auch kriminelle Akteure, mit hochprofessionellen Strukturen, sind auch in Deutschland aktiv, um Informationen und Daten zu erlangen oder Unternehmen zu erpressen. Gerade die Wirtschaftskriminalität hat sich zu einem lukrativen Geschäftsfeld entwickelt.

Der Digitalverband Bitkom schätzt allein den durch Datendiebstahl, Sabotage und Spionage entstandenen jährlichen Gesamtschaden zuletzt auf 223 Milliarden Euro – und dies nur in Deutschland.(1) Verbunden sind damit direkte Auswirkungen auf legale Wirtschaftstreibende und eine Gefährdung der Arbeitsplätze am Standort Deutschland.

Die durch Cyberkriminalität verursachten Schäden werden für Unternehmen und ihre Versicherer immer signifikanter. Zu diesem Schluss kommt eine Analyse der Allianz-Industrieversicherungstochter AGCS, die 1.736 Cyber-Schadensmeldungen aus den Jahren 2015 bis 2020 ausgewertet hat. Der Gesamtschaden lag laut AGCS bei 660 Millionen Euro.(2) Die Problematik bei der Cyberkriminalität besteht unter anderem darin, dass die Täter nahezu von jedem Ort der Welt aus agieren und ihre Spuren gut verschleiern können, da ein Tatort nicht zwingend mit dem Taterfolgsort identisch sein muss.

In den vergangenen Jahren ist die Professionalität der Täter deutlich gestiegen. Cyberangriffe auf ausgewählte Ziele werden akribisch vorbereitet und können erhebliche Folgen für die Wirtschaft und das Allgemeinwohl mit sich bringen.

Hierzu zählen Angriffe auf (kritische) Infrastruktur-einrichtungen und systemrelevante Unternehmen. Insgesamt führen externe und interne Faktoren zu großem Schaden für Unternehmen und den Wirtschaftsstandort Deutschland. Die durch die politischen Akteure initiierten Maßnahmen sind nicht ausreichend, um einen angemessenen Schutz der deutschen Wirtschaft zu gewährleisten und Arbeitsplätze zu schützen. Ziel muss sein, eine Resilienz der deutschen Wirtschaft zu erreichen. Aus Sicht des ASW Bundesverbandes besteht dringender Handlungsbedarf und ein klares Bekenntnis der Politik für den Wirtschaftsschutz!

(1) Vgl. Bitkom: Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, 2021, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr [19.08.2021]

(2) Vgl. AGCS: Allianz: Cyberkriminalität verursacht höchste Verluste für Unternehmen, aber interne Fehler führen am häufigsten zu Versicherungsschäden,2020 https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2020-de.html [08.07.2021]

Risiken und Herausforderungen für die Sicherheit in der Wirtschaft

Steigende Herausforderungen durch Digitalisierung von Wirtschaft und Gesellschaft

Der Begriff Digitalisierung feiert seit Jahren seinen Siegeszug durch sämtliche Bereiche der Gesellschaft und hat sich inzwischen zu einem Sammler unterschiedlichster Unternehmen entwickelt. Daten, Technologie, Produktmanagement, Menschen und Innovation sind die Kernelemente einer digitalen Transformation. In vielen Branchen hat die Digitalisierung schon jetzt zu einem tiefgreifenden Wandel geführt: der größte Einzelhändler der Welt hat keine Waren (Alibaba Group), das weltweit größte Taxiunternehmen besitzt keine Fahrzeuge (Uber), der größte Übernachtungsanbieter besitzt keinerlei Immobilien (Airbnb) und das größte Medienunternehmen erstellt keine Inhalte (Facebook).

Auch die deutsche Wirtschaft befindet sich im Prozess einer digitalen Transformation. Durch unterschiedliche nationale Regulierungen stellt dies insbesondere für global vernetzte Unternehmen eine große Herausforderung dar. Auch nach Einführung des IT-Sicherheitsgesetzes im Jahr 2015 hat sich die Cyber-Bedrohungslage trotz erheblicher Anstrengungen seitens Wirtschaft, Wissenschaft und des Staates weiter verschärft. Abwehrmaßnahmen und Sicherheitsinformationstechnologie haben nicht Schritt gehalten mit den erfolgten Cyberangriffen und deren Evolution.

Für Kriminelle, wie auch für fremde Nachrichtendienste sind Cyberangriffe über das Internet hochattraktiv, da eine Vielzahl von Schwachstellen in Soft- und Hardwareprodukten permanent neue Ansatzpunkte für die Entwicklung von Schadprogrammen liefern und durch die Möglichkeiten der Anonymisierung die Zurechenbarkeit von Angriffen erschwert wird.

Unsere Gesellschaft hat ein vitales Interesse an sicheren und resilienten Wirtschaftsunternehmen – und dies beschränkt sich nicht nur auf Betreiber kritischer Infrastrukturen und deren Aufgaben für die öffentliche Daseinsvorsorge, sondern auch Unternehmen mit hohem Schadenspotential bei Unfällen (z.B. durch Entweichen von Giften) als auch Unternehmen, deren wirtschaftlicher Erfolg entscheidend für das Prosperieren unserer Volkswirtschaft ist.

Cybersicherheit ist ein entscheidender Erfolgsfaktor, da nur ein notwendiges Maß an Sicherheit für Anwender und Kunden Vertrauen in Digitalisierung schafft. Deshalb hat auch die Industrie ein sehr hohes Eigeninteresse, ihre IT-Systeme abzusichern – nicht zuletzt, um die eigene wirtschaftliche Leistungs- und Wettbewerbsfähigkeit sicherzustellen.

Im Rahmen der Digitalisierung von Gesellschaft und Wirtschaft hat sich das Rollenverständnis von Staat und Wirtschaft gewandelt. Es ist erforderlich, dass der Staat angesichts der Bedeutung von Cybersicherheit stärkere Verantwortung in der Abwehr übernimmt, und dass gleichzeitig die Fähigkeiten der Anwender zur Selbstverteidigung durch Hilfe zur Selbsthilfe verbessert werden. Daher begrüßen wir generell die Zielsetzung der Bundesregierung die Cyberresilienz für den Wirtschaftsstandort Deutschland zu erhöhen.

Auch die Sicherheitsbranche befindet sich inmitten eines Veränderungsprozesses. Deutlich wird dies durch eine zunehmende Verschiebung von Sicherheitsbedrohungen aus dem analogen in den digitalen Raum. Dies geht Hand in Hand mit der Nutzung neuer digitaler Technologien zur Mitigation der neuen digitalen Bedrohungsformen. Waren früher eher physische Vermögenswerte, wie Navigationsgeräte in der Automobilherstellung, ein lohnendes Diebstahlsziel, stehen heute vermehrt digitale Werte, wie Kundendaten im Fokus des kriminellen Interesses. Für Sicherheitsunternehmen und Konzernsicherheiten gilt es mit dieser Entwicklung nicht nur Schritt zu halten, sondern ihr vielmehr einen Schritt voraus zu sein.

Steigende Herausforderungen durch Digitalisierung von Wirtschaft und Gesellschaft

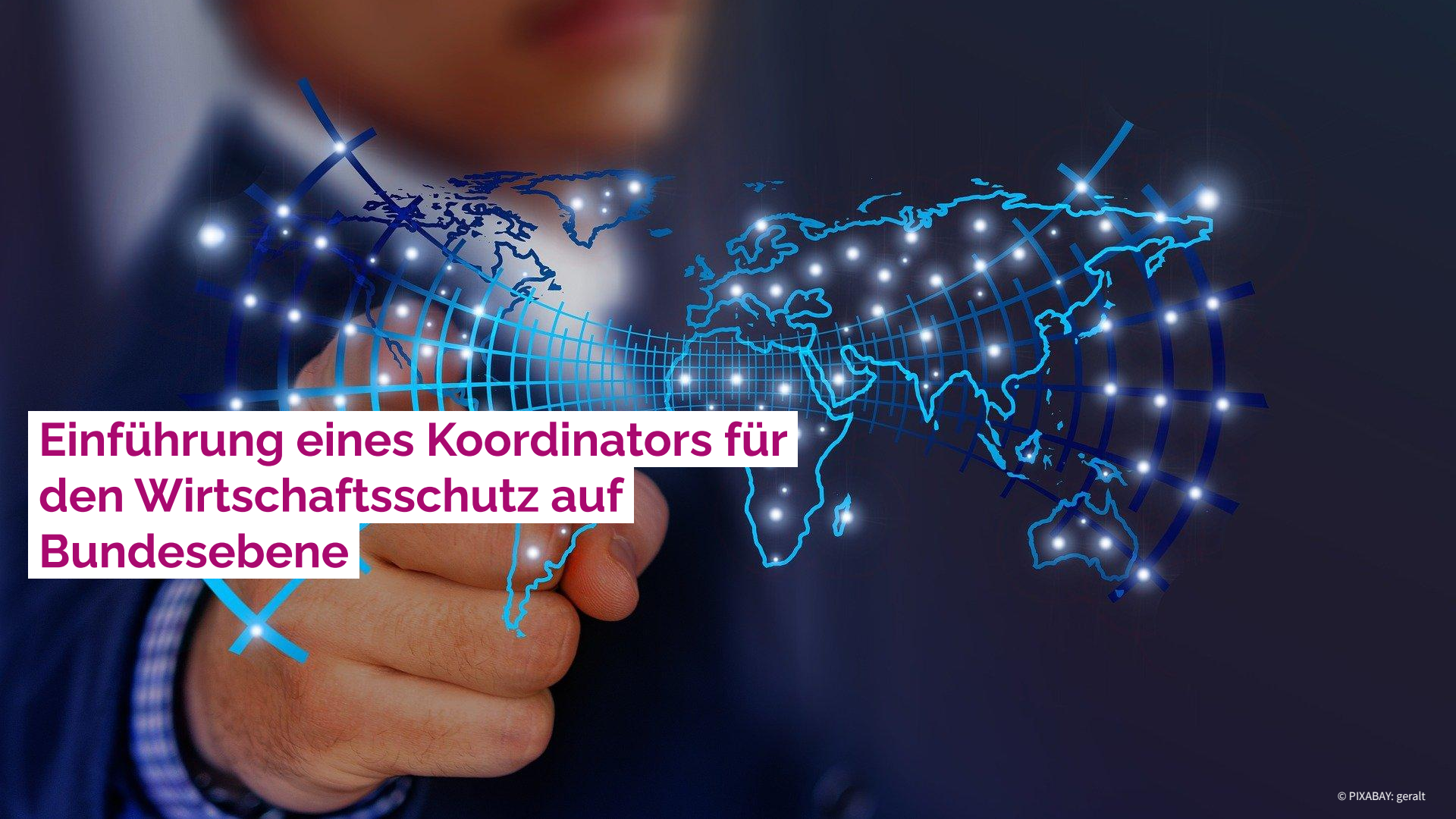
Im Sicherheitsbereich wird das Thema Digitalisierung schnell mit Cyber-Sicherheit gleichgesetzt. Das greift jedoch zu kurz. Digitalisierung umfasst weit mehr als Technologie und fordert ein neues Denken, den Einsatz und die selbstverständliche Nutzung von Technologien und agilen Arbeitsmethoden.

Mit der Entstehung neuer Angriffsvektoren aus dem Cyber-Raum nimmt die Bedeutung der Cyber-Sicherheit beständig zu. So finden Betrug, Erpressung, Diebstahl, Anschläge nicht nur im physischen, sondern immer öfter im Cyberraum statt. Als Beispiel seien hier der CEO-Fraud genannt, Phishing Mails, eine Erpressung mit Bitcoin-Forderungen, DDOS-Attacken auf die Webseiten von Firmen, sog. „Fake News", die erst durch soziale Medien ihre Wirkung entfalten. Die Konsequenz daraus ist: eine Verlagerung von der physischen in die digitale Welt. Veränderungen, denen sich die gesamte Sicherheitsbranche kompromisslos stellen muss.

Der stärkere Fokus auf Bedrohungen aus dem digitalen Raum hat seine Berechtigung, trotzdem sollten die Auswirkungen auf klassische Sicherheitsthemen nicht außer Acht gelassen werden. Auch diese Bereiche müssen sich neuen Bedrohungen resultierend aus der Digitalisierung stellen und können dies mit digitalen Lösungen effektiver und effizienter als bisher tun. Nicht zu vergessen: auch in der IT-Sicherheit spielt physische Sicherheit eine wichtige Rolle. Sie spielt Hand in Hand mit der digitalen, ergänzt und unterstützt diese wirkungsvoll, wie beispielsweise der Perimeterschutz um ein Datenzentrum.

Ziel muss es sein, einen strategischen, umfassenden und vernetzten Wirtschaftsschutz zu etablieren. Dieser muss über das IT-Sicherheitsgesetz hinausgehen und darf sich nicht allein auf IT-bezogene Maßnahmen fokussieren. Er umfasst auch organisatorische und personelle Schutzmaßnahmen. Ein enger und vertrauensvoller Erfahrungsaustausch zwischen staatlichen Stellen und Unternehmen ist Basis für einen erfolgreichen Wirtschaftsschutz.

Einführung eines Koordinators für den Wirtschaftsschutz auf Bundesebene



Deutschland im Fokus von kriminellen Akteuren und fremden Nachrichtendiensten

Der Technologiestandort Deutschland ist mit seiner Unternehmenslandschaft zunehmenden Risiken durch Wirtschafts- bzw. Industriespionage ausgesetzt. Spionageaktivitäten stellen eine reale Bedrohung für deutsche Unternehmen dar. Dabei sind drei Kategorien von Geschäftsgeheimnissen, die besonders schützenswert sind, hervorzuheben: Forschungsdaten, Produktspezifikationen und Fertigungstechnologien. Deren Attraktivität liegt meist in einem spezifischen Entwicklungsverfahren, einer herausragenden Qualität oder einer Fertigung mit deutlich besserer Kosteneffizienz im Vergleich zu den Wettbewerbern.

Abflüsse von Know-how bedrohen Unternehmen nicht nur außerhalb der Landesgrenzen, sondern auch im Inland. Dabei agieren einerseits wirtschaftliche Konkurrenten, andererseits Nachrichtendienste fremder Staaten, die die gewonnenen Informationen zu Gunsten der heimischen Wirtschaft oder strategischen/militärischen Vorteilen verwerten. Neben reinen Wettbewerbsnachteilen kann Wirtschafts- und Industriespionage massive wirtschaftliche Schäden verursachen, berücksichtigt man die Tatsache, dass sich enorme Forschungs- und Entwicklungskosten nicht amortisieren können, weil der Wettbewerb sich Aufwand durch Einsatz von Spionage gespart hat und im Ergebnis deutlich günstiger produzieren und am Markt anbieten kann.

Auch die Produktpiraterie bringt in diesem Kontext eine massive Gefährdung mit sich. Dies geht weit über die in zahlreichen Urlaubsländern angebotenen gefälschten Uhren und T-Shirts hinaus. Zunehmend werden auch komplexe Anlagen und Maschinen exakt kopiert, so dass die Unterscheidung zwischen echt und falsch selbst den Herstellern schwerfällt. Hieraus ergeben sich Umsatzeinbußen durch Kunden, die gefälschte Ware anstatt des Originals erwerben, Reputationsschäden durch Vertrauensverlust in renommierte Marken sowie Haftungsrisiken aufgrund der mangelnden Unterscheidungsmöglichkeiten zwischen Original und Fälschung.(3)

Bedingt durch die fortschreitende Globalisierung wird sich der Wettbewerb weiter verschärfen und die Aktivitäten von fremden Nachrichtendiensten und kriminellen Akteuren weiter zunehmen.

Der Verlust von geschäftsrelevanten Informationen kann bei Unternehmen zu massiven Wettbewerbsnachteilen, zu Einschränkung von Kundenvertrauen, Reputationsschäden und im schlimmsten Fall zum Bankrott führen. Ohne die erforderlichen Gegenmaßnahmen wird es zu signifikanten Schäden für den Wirtschaftsstandort Deutschland kommen.

(3) Vgl. Fedder, Felix Ole et al.: „Wirtschaftskriminalität", in: Globale Herausforderungen. Chancen und Risiken für unsere Zukunft, Security Explorer, 2013, S. 263-306.

Wirtschaftskriminalität nimmt zu

Wirtschaftskriminalität hat sich weltweit zu einem hochprofitablen Modell entwickelt. Mit Einzug der Digitalisierung und der stetig wachsenden Vernetzung von IT-Systemen werden auch permanent neue Wege und die Mittel erarbeitet, mit denen sich Kriminelle Zugang zu Netzwerken, Daten und Informationen verschaffen. Speziell das Internet spielt als Tatort eine große Rolle und wird als Mittel für die Begehung von Straftaten instrumentalisiert. Der Grad der Professionalisierung von Kriminellen wächst kontinuierlich. Das Umfeld der kriminellen Akteure ist komplex und zwischenzeitlich hochprofessionell organisiert. Grenzüberschreitende Kriminalität sowie unterschiedliche Rechtsordnungen stellen die Strafverfolgungsbehörden vor massive Herausforderungen, die mit den derzeitigen (rechtlichen) Rahmenbedingungen nahezu nicht mehr bewältigt werden können.

Das Bundeskriminalamt verzeichnet in seinem Lagebild Wirtschaftskriminalität 2019 zwar einen Rückgang der Fallzahlen. So wurden laut dem Bundeslagebild im Berichtsjahr 40.484 Fälle mit einer Schadenssumme in Höhe von 2,973 Mrd. Euro registriert.(4) Es ist jedoch davon auszugehen, dass rund 80 Prozent im Bereich der Wirtschaftskriminalität dem Dunkelfeld unterliegen. Gerade vor dem Hintergrund möglicher Reputationsschäden zeigen Unternehmen Straftaten, die der Wirtschaftskriminalität zuzuordnen sind, häufig nicht an.

Laut einer KPMG-Studie aus dem Jahr 2020 begangen externe Täter in 47% der Fälle die kriminellen Handlungen. Bei 10 Prozent der Fälle haben externe und interne Täter die Taten gemeinschaftlich durchgeführt.(5) D.h. in zahlreichen Fällen werden die wirtschaftskriminellen Handlungen durch Innentäter verursacht, wobei auch Unachtsamkeit und Nachlässigkeit eine hohe Relevanz haben. Allerdings werden auch häufig Mitarbeiter durch „Social Engineering“ und „Social Hacking“ instrumentalisiert.

Auch bei besten IT-Sicherheitssystemen und internen Kontrollen bleibt der Mensch eine wesentliche Schwachstelle. Im Kontext von „Social Engineering“ wird in zahlreichen Fällen das Umfeld des Opfers ausgespäht, falsche Identitäten eingesetzt sowie konkrete Verhaltensweisen (z.B. Autoritätshörigkeit) ausgenutzt, um an die gewünschten Informationen zu gelangen.

Die Täter bedienen sich gängiger Plattformen wie beispielsweise XING, Facebook, LinkedIn, um an die erforderlichen Daten der Opfer zu kommen.(6)

(4) Vgl. BKA: Wirtschaftskriminalität – Bundeslagebild 2019, 2020, S. 6-8.
(5) Vgl. KPMG: Im Spannungsfeld – Wirtschaftskriminalität in Deutschland 2020, 2020, S. 18.
(6) Vgl. Fedder, Felix Ole et al.: „Wirtschaftskriminalität“, in: Globale Herausforderungen. Chancen und Risiken für unsere Zukunft, Security Explorer, 2013, S. 263-306.

Regelmäßiger Austausch auf höchster Ebene

Extremismus als Risiko für die deutsche Wirtschaft

Der Umgang mit zunehmender Radikalisierung und Populismus ist eine gesamtgesellschaftliche Herausforderung. Vor allem die schleichende Entgrenzung zwischen legitimen bürgerlichen Protest und extremistischen Strömungen bietet Anlass zur Wachsamkeit.

Das Bundesamt für Verfassungsschutz zählt in seinem Verfassungsschutzbericht aus dem Jahr 2020 zwischenzeitlich ein Personenpotenzial von 33.300 Rechts-, 34.300 Linksextremen sowie 28.715 Islamisten. Eine hohe Anzahl wird als gewaltbereit eingestuft.(7) Auch die deutsche Wirtschaft muss sich zunehmend auf extremistische Protestformen einstellen.

Radikalisierungstendenzen und extremistische Einflüsse auf Mitarbeiterinnen und Mitarbeiter können aber auch im Unternehmen erkennbar werden. Hier sind Unternehmen zwischen Personalverantwortung und Sicherheitsanforderungen an gleich mehreren Stellen gefordert, passende Antworten gemeinsam mit den Sicherheitsbehörden zu entwickeln. Fünf Entwicklungen haben für die deutsche Wirtschaft eine hohe Relevanz:

1. Gewaltsame Angriffe: Die deutsche Wirtschaft ist immer wieder direkt von Extremismus betroffen. Dies zeigen zahlreiche Brandanschläge auf Firmenwagen und Geschäftseinrichtungen von Unternehmen in den letzten Jahren.

2. Protestaktionen: Die Grenzen zwischen bürgerlichen Interessensbekundungen und extremistischen Handlungen sind fließend. Die freie Meinungsäußerung ist ein Grundpfeiler der Demokratie und wichtig für die Gesellschaft. Allerdings steigt die Bereitschaft zu mutwilligen und gewalttätigen Aktionen auch gegen Unternehmen, wobei neben Eigentums- auch Körperverletzungen in Kauf genommen werden.

3. Radikalisierung von Mitarbeitern: Mitarbeiter von Unternehmen können sich radikalisieren. Extremistische Ideologien können so zu einer Gefahr für den Betriebsfrieden werden. Zum Beispiel entfalten Sympathisanten erheblichen missionarischen Eifer, der Einfluss auf Mitarbeiter und Betriebsklima haben kann. Denkbar ist auch, dass Insiderwissen für ideologisch motivierte Sabotageaktionen missbraucht werden kann.

4. Reputationsschaden: Schaden für den Ruf eines Unternehmens kann entstehen, wo dieses nicht nur legitim in der Öffentlichkeit kritisiert, sondern – verstärkt durch soziale Medien – Ziel von professionellen Boykott- bzw. Shitstorm-Kampagnen wird.

5. Kollaterales Ausmaß: Extremisten fokussieren sich nicht auf bestimmte Branchen. Gerade globale oder internationale Veranstaltungen von Wirtschaft oder Politik werden regelmäßig von massiven, auch extremistisch motivierten Protesten und Ausschreitungen begleitet, welche die lokale Wirtschaft ob ihrer rufschädigenden Wirkung als attraktiven Standort für weitere Investitionen in Mitleidenschaft ziehen können.

Nur durch gemeinsame Anstrengungen von staatlichen Stellen und Privatwirtschaft, können extremistische Tendenzen in der Belegschaft identifiziert und Aktivitäten gegen die Unternehmen verhindert werden.

(7) Vgl. BMI: Verfassungsschutzbericht 2020, 2020, S. 53, 125, 196.

Zunahme von Naturkatastrophen und externen Ereignissen als Bedrohung für den Wirtschaftsstandort Deutschland

Pandemien, Extremwetterereignisse und Katastrophen werden künftig verstärkt auftreten und Auswirkungen auf den Standort Deutschland sowie die Welt haben. Ausfall von Lieferketten und Mitarbeitenden, Betriebsunterbrechungen sowie die Folgen von Unruhen und Protesten stellen ein hohes Risiko für die Unternehmen dar.

Viele Wirtschaftsbetriebe sind auf heutige und zukünftige Szenarien nur unzureichend vorbereitet. Ein weiteres Problem ergibt sich durch die schlechte Einbindung der Unternehmen in staatliche Strukturen – beispielsweise in die kommunale Pandemieplanung oder den Informationsaustausch von behördlichen Lagezentren (z.B. das Gemeinsame Melde- und Lagezentrum von Bund und Ländern).

Ohne die Privatwirtschaft, speziell die Unternehmen aus den sogenannten systemrelevanten Bereichen, kann die Versorgung der Bevölkerung mit lebensnotwendigen Gütern und Dienstleistungen bei Schadenslagen und Katastrophen nicht aufrechterhalten werden.

Auch der Ausfall von (einzelnen) Sektoren der Kritischen Infrastruktur führt unweigerlich zu Versorgungsengpässen und so zu erheblichen Konsequenzen für die Innere Sicherheit.

Sonderthema Geheimschutz

Die geheimschutzbetreute Wirtschaft leistet einen großen Beitrag zur nationalen Sicherheit der Bundesrepublik Deutschland. Die beim Bundesministerium für Wirtschaft und Energie (BMWi) angesiedelte Zuständigkeit für die Geheimschutzbetreuung bedarf insgesamt einer Stärkung und Modernisierung.

Seit der Novellierung des Sicherheitsüberprüfungsgesetz (SÜG) im Jahr 2017 geht das BMWi dazu über, sich aus der Geheimschutzbetreuung zurückzuziehen und die notwendigen Aufgaben auf die öffentlichen Auftraggeber zu verlagern, die diese aber teilweise nicht angemessen wahrnehmen können. Firmen erleiden hierdurch Wettbewerbsnachteile. Insbesondere aber werden der Schutz staatlicher Verschlusssachen, und damit die nationale Sicherheit geschwächt, da die Unternehmen keiner diesbezüglichen Steuerung und Kontrolle mehr unterliegen.

Auch die Digitalisierung macht vor der Verarbeitung von Verschlusssachen nicht halt. Unternehmen erhalten jedoch nur geringe Unterstützung von staatlicher Seite zur Implementierung adäquater Schutzmechanismen auf der Basis zugelassener IT. Der diesbezügliche Beratungsauftrag des BSI richtet sich nur an die öffentliche Verwaltung. Mangelnde Unterstützung der Wirtschaft in den komplexen Vorgaben des IT-Geheimschutzes führt zu Sicherheitsverlusten und Effizienznachteilen.

IT-Lösungen zur Bearbeitung von VS auch niedrigster Einstufung sind nur beschränkt verfügbar, teuer und nicht in moderne Unternehmen integrierbar. Dies führt zur Schaffung von teuren parallelen IT-Welten, wo Industriestandards bereits äquivalente Sicherheit bieten könnten.

Positionen, Forderungen und Handlungsempfehlungen

Um die deutsche Wirtschaft sicherer zu machen, sind verschiedene Maßnahmen zu initiieren. Der ASW Bundesverband positioniert sich mit Blick auf die zukünftige Bundesregierung mit folgenden Handlungsempfehlungen und Forderungen:

Einführung eines Koordinators für den Wirtschaftsschutz auf Bundesebene

Sicherheit ist das Fundament für Innovation, Durchsetzungskraft und Erfolg unserer Wirtschaft. Diese Sicherheit ist unsere gemeinsame Verantwortung. Um Verantwortung wahrzunehmen, benötigen wir ein „Gesicht für den Wirtschaftsschutz" auf Bundesebene. Der ASW Bundesverband fordert die Ernennung eines Koordinators für Wirtschaftsschutz. Dieser soll die Zuständigkeiten auf Bundesebene koordinieren, die Vernetzung von Bundesakteuren mit regionalen und kommunalen Stakeholdern aus Behörden, Verbänden, deren Mitgliedsunternehmen und Forschungseinrichtungen verstetigen, behördenübergreifende Detektion besonders gefährdeter Branchen aufbauen und als politischer Motor für umfassenden Wirtschaftsschutz agieren.

Jährliches Strategiegespräch auf höchster Ebene

Um den effizienten Austausch auf höchster Ebene zu gewährleisten, fordert der ASW Bundesverband einmal pro Jahr ein Treffen auf Staatssekretärs-Ebene bzw. mit dem Koordinator für Wirtschaftsschutz sowie den Vorsitzenden der beteiligten Wirtschaftsschutzverbände im Rahmen des Steuerungskreises der Initiative Wirtschaftsschutz. Gesprächsgegenstand wären Status quo sowie die strategische Entwicklung.

Transparenz über die aktuelle Gefährdungslage durch Einrichtung einer Analyse- und Strategieplattform

Ein Informationsaustausch zwischen staatlichen Stellen und privatwirtschaftlichen Einrichtungen ist nur marginal und/oder basierend auf persönlichen Kontakten oder regionalen Sicherheitspartnerschaften vorhanden. Eine institutionalisierte Kooperation zur Bewältigung komplexer Ereignisse oder zur gemeinsamen Lagebewertung existiert nicht. Systemrelevante- und KRITIS-Unternehmen sind auf die Erkenntnislage der Sicherheitsbehörden angewiesen.

Es ist zwingend erforderlich, geeignete Kommunikationswege (auch für eingestufte Informationen) zu schaffen, um Unternehmen präventiv über Angriffe auf Unternehmen bzw. Branchen zu unterrichten.

Der ASW Bundesverband fordert die Einrichtung einer Nationalen Analyse- und Strategieplattform für Wirtschaftsschutz. Nur durch eine interdisziplinäre und ressortübergreifende Schnittstelle zwischen Vertretern von Sicherheitsbehörden und Unternehmen kann ein realistisches (Bundes-) Gefährdungslagebild und effektive branchenspezifische Schutzkonzepte, Standards zur Stärkung einer sicheren und nachhaltigen Wertschöpfungs-/Lieferkette für Unternehmen (insbesondere KMU) sowie Forschungseinrichtungen erarbeitet werden.

Auf Basis agiler Prozessstrukturen sorgt diese Plattform für einen permanenten, beidseitigen Informationsfluss zu akuten und künftigen Bedrohungslagen, eine Hotline dient als Anlaufstelle für akute Vorfälle.

Regionale Sicherheitspartner-schaften nutzen und Wirtschaftsschutz auf kommunaler Ebene etablieren

Der Wirtschaftsschutz muss dort etabliert werden, wo die Wirtschaft tätig ist. In vielen Regionen gibt es bereits Sicherheitspartnerschaften zwischen den Landessicherheitsbehörden, den Industrie- und Handelskammern und den ASW/VSW Regional-/Landesverbänden – zumeist unter Schirmherrschaft der Innenministerien der Länder.

Ein flächendeckender Ausbau regionaler Sicherheitspartnerschaften ist erforderlich.

Der ASW Bundesverband fordert, die Sicherheitspartnerschaften auszubauen und die Aktivitäten unter der „Initiative Wirtschaftsschutz" zu bündeln. Für die stärkere Einbindung, speziell von kleineren und mittleren Unternehmen, sind die öffentlichkeitswirksamen Maßnahmen (z.B. in Form von Kampagnen) notwendig.

Internationalisierung: Kooperation mit Partnerländern ausbauen

Wirtschaft ist global und nicht auf Deutschland begrenzt. Auch Angreifer agieren global. Deshalb sollte beim Wirtschaftsschutz nicht zwischen Ausland und Inland differenziert werden. Um auf den internationalen Märkten als Global Player agieren zu können, benötigt die deutsche Wirtschaft einen Ausbau internationaler Zusammenarbeit im Wirtschaftsschutz.

Eine stabile, global verflochtene Wirtschaft bietet nicht nur Basis für freiheitliche Demokratie und gesellschaftlichen Zusammenhalt, sondern auch die Grundlage für deutsches politisches Engagement weltweit. Daher setzt sich der ASW Bundesverband für ein starkes Schutzschild für Industrie, Handel, Dienstleistungen und unsere zentralen Wertschöpfungs- und Lieferketten ein.

Die globale Verflochtenheit fordert eine enge Kooperation mit unseren weltweiten Partnern, zur gemeinsamen strategischen Abstimmung und dem Austausch von Best Practices. Weitere Partner (z.B. das Auswärtige Amt) sind für diese Zielsetzung einzubinden.

Stärkung Geheimschutz / Geheimschutz-betreuung

Die Geheimschutzbetreuung des Bundes für Wirtschaftsunternehmen muss zentral erhalten bleiben und gestärkt werden. Aufgaben, wie die Sicherheits- und Zuverlässigkeitsüberprüfungen, müssen effizient konsolidiert und in einem Ressort zusammengefasst werden.

Die Geheimschutzbetreuung des Bundes muss mit dem Wirtschaftsschutz verzahnt werden.

Das BSI sollte Firmen in Beschaffung und Betrieb von VS-technischen Systemen beraten.

Transparenz über die aktuelle Gefährdungslage

Aufklärung von Wirtschaftsspionage als expliziter Bestandteil des sicherheitsbehördlichen Auftrags

Die Spionageabwehr gehört zum Auftrag der Nachrichtendienste der Bundesrepublik Deutschland. Ein Auftrag zur Abwehr von Wirtschaftsspionage geht aus dem gesetzlichen Auftrag nicht klar hervor. Der ASW Bundesverband fordert die Aufklärung von Aktivitäten fremder Mächte zum Nachteil von Wissenschaft und Wirtschaft gesetzlich zu regeln.

Der Schutz von Wirtschaft und Wissenschaft vor Spionage und Sabotage durch staatliche Akteure muss expliziter Bestandteil des sicherheitsbehördlichen Auftrags werden.

Darüber hinaus sind im Interesse eines resilienten Wirtschafts- und Wissenschaftsstandortes bei Gesetzgebungsvorhaben, Forschungsplanungen und -projekten sowie Kooperationen im Bereich Wirtschaft und Wissenschaft die Belange des Know-how-Schutzes, der Einflussnahme und der Unternehmenssicherheit von Beginn mit einzubeziehen.

Hierzu empfiehlt sich die Einrichtung eines anlassbezogenen Security Boards mit den sicherheitsbehördlichen und verbandsseitigen Partnern der Initiative Wirtschaftsschutz.

Unternehmen für den Wirtschaftsschutz befähigen

Erfolgreiche Angriffe auf den deutschen Mittelstand resultieren in der Regel aus Schwächen im Basisschutz. Das Spektrum reicht von unzureichendem Schutz von Vermögensgegenständen bei Transport und Lagerung bis hin zu nicht durchgeführten Software-Updates bei kritischen IT-Systemen sowie schwachen Passwörtern.

Daher sieht der ASW Bundesverband den Ausbau des Wirtschaftsgrundschutzes als zwingend erforderlich an. Lösungen stellen die einfach umzusetzenden Maßnahmen im Wirtschaftsgrundschutz dar. Das Projekt „Wirtschaftsgrundschutz“ ist ein Erfolgsbeispiel für die übergreifende Zusammenarbeit.

Es wird getragen von der partnerschaftlichen Kooperation der Projektpartner Bundesamt für Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik, der HiSolutions AG und des ASW Bundesverband und liefert als Ergebnis konkrete, praxisorientierte Hilfestellungen für die deutsche Wirtschaft.

Es hat den Anspruch, sowohl kleinen und mittelständischen Unternehmen als auch Großunternehmen, Hinweise und Optionen aufzuzeigen, wie konkrete Einzelbedrohungen bewältigt werden können und das Gesamtthema effektiv gesteuert wird. Der ASW Bundesverband fordert eine Fortsetzung und Ausweitung des Projekts.

Dafür ist die Bereitstellung öffentlicher Mittel erforderlich.

Über den ASW Bundesverband

Der ASW Bundesverband (Allianz für Sicherheit in der Wirtschaft e.V.) vertritt die Sicherheitsinteressen der deutschen Wirtschaft auf Bundesebene.

Er schafft Bewusstsein für das Thema Wirtschaftsschutz – bei den Unternehmen, der Politik und in den Medien. Er sorgt für einen Informationsaustausch – kontinuierlich und anlassbezogen – zwischen Unternehmen und den Sicherheitsbehörden und stellt den Unternehmen aufbereitete Informationen zur Verfügung.

Der Verband schafft ein verlässliches Netzwerk, führt Lehrveranstaltungen sowie Expertenworkshops durch und ist zusammen mit dem Bundesamt für Verfassungsschutz (BfV) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Herausgeber des Wirtschaftsgrundschutz-Handbuches.

Die Mitglieder des ASW Bundesverbandes sind acht regionale Verbände für Sicherheit in der Wirtschaft und vier Fachverbände. Der Verband ist darüber hinaus Partner der Initiative Wirtschaftsschutz.

Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6
10779 Berlin

+49 (0)30 2463 7175
www.asw-bundesverband.de

ASW Bundesverband