Verteidigungsfähigkeit braucht praxistauglichen Geheimschutz

Vorschläge zur Modernisierung von Geheimschutz und Sicherheitsüberprüfungen

bitkom

Ausgangslage

Geheimschutz und Sicherheitsüberprüfungen sind für die Lieferfähigkeit der Digitalwirtschaft im Bereich der Sicherheit und Verteidigung zentral. Für Unternehmen sind die Verfahren jedoch häufig langwierig, schwierig planbar und nicht ausreichend auf digitale Prozesse ausgerichtet. Insbesondere für neue Marktakteure, die erstmals in sicherheits- oder verteidigungsrelevante Projekte einsteigen, ist der Zugang erschwert.

Bitkom-Bewertung

Die Richtung stimmt: Das Sicherheitsüberprüfungsgesetz im Jahr 2025 war ein wichtiger Schritt, um Verfahren an die veränderte sicherheitspolitische Lage anzupassen. In der praktischen Umsetzung bestehen weiterhin Hürden für Unternehmen. Geheimschutz und Sicherheitsüberprüfungen müssen einfacher, digitaler und damit praxistauglicher werden. Dadurch sollen Verfahren beschleunigt werden, ohne Sicherheitsstandards abzusenken.

Das Wichtigste

Damit der Geheimschutz für Unternehmen und Behörden sicher und schnell umsetzbar ist, braucht es aus Sicht des Bitkom vor allem drei Dinge:

- **Zugang erleichtern: Orientierung, Vorbereitung und klare Anforderungen schaffen**

  Unternehmen brauchen frühzeitig verständliche Informationen zu Abläufen, Zuständigkeiten und planbaren Maßnahmen. Das Geheimschutzhandbuch muss modernisiert und durch digitale Angebote, etwa Schulungsvideos oder Handreichungen, ergänzt werden.

- **Verfahren harmonisieren: Anerkennung stärken und Doppelstrukturen vermeiden**

  Bereits erfolgte Sicherheitsüberprüfungen sollten stärker behördenübergreifend sowie bund- und länderübergreifend anerkannt werden. Unternehmen brauchen eine koordinierende Stelle, die Verfahren bündelt, Doppelaufwand reduziert und Geheimschutzanforderungen ganzheitlicher betrachtet.

- **Effizienz stärken: Verfahren digitalisieren und Einsatzmöglichkeiten flexibilisieren**

  Die Aufnahme in die Geheimschutzbetreuung und damit verbundene Sicherheitsüberprüfungen müssen medienbruchfrei digitalisiert und durch ausreichende Ressourcen unterstützt werden. Zugleich sollte es einfacher werden, geprüfte Personen in VS-Aufträgen einzusetzen.

Einleitung

Angesichts zunehmender hybrider Bedrohungen, wachsender Cyberrisiken und der veränderten sicherheitspolitischen Lage ist die Liefer- und Anpassungsfähigkeit der Sicherheits- und Verteidigungswirtschaft von zentraler Bedeutung für die Verteidigungsfähigkeit Deutschlands. Damit gewinnt die Frage an Bedeutung, wie Unternehmen erhöhte Geheimschutzanforderungen erfüllen und Zugang zu entsprechenden Projekten erhalten können. Gleichwohl stammen zahlreiche Lösungsansätze des Geheimschutzes noch aus einem vordigitalen Verständnis von Sicherheit. Sie tragen digitalen Prozessen, aktuellen Bedrohungslagen sowie international agierenden Zulieferern und vernetzten Wirtschaftsstrukturen bislang nicht ausreichend Rechnung.

Eine zentrale Voraussetzung für Unternehmen, um im sicherheits- und verteidigungsrelevanten Umfeld tätig zu werden, ist häufig die Aufnahme in die Geheimschutzbetreuung. Ohne diese ist eine Teilnahme an Ausschreibungen oder die Mitarbeit an entsprechenden Projekten vielfach nicht möglich. Ihre Einleitung kann jedoch in der Regel nur über einen Bedarfsträger erfolgen. Damit bestimmt die Geheimschutzbetreuung maßgeblich, ob und wann Unternehmen sicherheitsrelevante Produkte und Dienstleistungen liefern können. Für Unternehmen, die neu in diesen Markt eintreten und schnell innovative Lösungen bereitstellen wollen, bedeutet das bereits früh eine hohe Zugangshürde.

Mit der Novellierung des Sicherheitsüberprüfungsgesetzes (SÜG) Ende 2025 hat der Deutsche Bundestag Anpassungen vorgenommen, um Verfahren an die veränderte sicherheitspolitische Lage anzupassen. Der Bitkom hat sich im Gesetzgebungsprozess dafür eingesetzt, Geheimschutzanforderungen und Sicherheitsüberprüfungen stärker mit den Bedürfnissen der Wirtschaft in Einklang zu bringen und praktikablere Verfahren zu schaffen.

Aktuelle Herausforderungen

Für Unternehmen, die erstmals mit sicherheits- oder geheimschutzrelevanten Anforderungen in Berührung kommen, fehlt häufig eine zentrale Anlaufstelle, die konkrete Orientierung bietet. Zwar existieren Informationsangebote wie das Geheimschutzhandbuch, diese werden jedoch nicht immer als ausreichend aktuell, praxisnah oder leicht zugänglich wahrgenommen. Dadurch bleiben geltende Anforderungen, notwendige Vorbereitungsmaßnahmen und zuständige Ansprechpartner für Unternehmen oftmals unklar.

Darüber hinaus erhalten Unternehmen vor einer formalen Aufnahme in die Geheimschutzbetreuung oftmals keinen Zugang zu Informationen, die für die rechtzeitige Umsetzung organisatorischer, personeller, technischer oder baulicher Anforderungen erforderlich sind. Dies erschwert eine vorausschauende Planung und kann die Aufnahme sicherheitsrelevanter Tätigkeiten verzögern.

Gleichzeitig führen lange Bearbeitungszeiten bei Sicherheitsüberprüfungen, häufig von mehreren Monaten, zu erheblichen Verzögerungen und Planungsunsicherheiten. Hinzu kommt, dass durchgeführte Sicherheitsüberprüfungen nicht immer behördenübergreifend anerkannt werden, was Doppelprüfungen und zusätzlichen Aufwand verursacht. Hohe »Durchfallquoten« der betroffenen Mitarbeiterinnen und Mitarbeiter machen das Personalmanagement komplex.

Neben dem Geheimschutz gewinnt auch der Sabotageschutz an Bedeutung, insbesondere für Unternehmen, die kritische Dienstleistungen oder Infrastrukturleistungen für Staat und Bundeswehr erbringen wollen. In der Praxis bestehen jedoch weiterhin Unsicherheiten bei Zuständigkeiten, Verfahren und der einheitlichen Auslegung durch verschiedene Behörden.

Zusammen mit der Notwendigkeit eines Bedarfsträgers zur Einleitung des gesamten Verfahrens entsteht daraus ein strukturelles Problem: Unternehmen können sich nicht proaktiv vorbereiten oder qualifizieren. Dadurch entstehen konkrete Wettbewerbsnachteile für innovative Unternehmen und die Lieferung neuer Technologien an den Bedarfsträger wird verzögert.

Handlungsempfehlungen

Um die Innovationsfähigkeit im sicherheits- und verteidigungsrelevanten Umfeld zu stärken und insbesondere neuen Akteuren den Marktzugang zu erleichtern, schlägt der Bitkom folgende Anpassungen vor:

1. Zugang verbessern

- **Modernisierung des Geheimschutzhandbuchs:** Das Geheimschutzhandbuch sollte grundlegend aktualisiert und regelmäßig gepflegt werden. Dabei sollten moderne Sicherheitsarchitekturen wie Zero Trust, fortgeschrittene Verschlüsselungs-standards und zeitgemäße Endgerätekonzepte stärker berücksichtigt werden. Ziel sollte es sein, überprüftem Personal ein effizientes Arbeiten mit modernen digitalen Werkzeugen zu ermöglichen, ohne zentrale Geheimschutzprinzipien wie Need-to-know, Netzisolierung und den Schutz von Verschlusssachen aufzuweichen.

  Ergänzend braucht es eine praxisnahe Handreichung für Unternehmen, die Anforderungen des Geheimschutzes verständlich erläutert und konkrete Orientierung für die Umsetzung in der Wirtschaft bietet.

- **Frühzeitige Information und Vorbereitung ermöglichen:** Mit dem Beginn der Aufnahme in die Geheimschutzbetreuung sollte seitens des Bundesministeriums für Wirtschaft und Energie (BMWE) ein standardisiertes Informationsangebot bereitgestellt werden. Inhalte sollten den allgemeinen Ablauf, anstehende Anforderungen sowie frühzeitig vorbereitbare organisatorische, personelle und bauliche Maßnahmen umfassen. Dies kann beispielsweise durch Schulungsvideos oder andere digitale Formate erfolgen.

- **Frühzeitige Prüfoptionen für sicherheitskritisches Personal schaffen**: Unternehmen, die einen Einstieg in sicherheits- oder verteidigungsrelevante Projekte planen, sollten für einen klar begrenzten Kreis zentraler Personen frühzeitig Prüfungen anstoßen können. Dies sollte auch in der Anbahnung einer Vertragsbeziehung mit einem Bedarfsträger möglich sein, sofern ein nachvollziehbarer sachlicher Bezug zu künftigen VS-Aufträgen, sicherheitskritischen Funktionen oder vergleichbaren Tätigkeiten besteht. Erfasst werden könnten insbesondere Geschäftsleitungen. Bereits vorhandene Compliance- oder Hintergrundprüfungen sollten dabei berücksichtigt werden können, um Verfahren zu beschleunigen und den Markteintritt planbarer zu machen. Da solche Überprüfungen einen Eingriff in Persönlichkeitsrechte, insbesondere in das Recht auf informationelle Selbstbestimmung darstellen, müssen sie gesetzlich eindeutig begrenzt und strikt am Verhältnismäßigkeitsprinzip ausgerichtet sein. Sie dürfen nur vorgesehen

werden, wenn sie für die jeweilige sicherheitskritische Funktion geeignet, erforderlich und angemessen sind.

- **Anwendungsbereich anpassen:** Der Anwendungsbereich sicherheitsbezogener Überprüfungen im Rahmen des vorbeugenden personellen Sabotageschutzes sollte sektorenübergreifend stärker an funktionalen Kritikalitätskriterien ausgerichtet werden, statt allein an starren Schwellenwerten. Maßgeblich sollten insbesondere Versorgungsrelevanz, mögliche Kaskadeneffekte und zentrale Steuerungsfunktionen sein. Dies wird insbesondere am Beispiel der Energiewirtschaft deutlich, da bestehende Schwellenwerte nicht immer die tatsächliche Relevanz einzelner Einrichtungen abbilden. So können Leitstellen von Elektrizitätsverteilernetzen für die Versorgung großer Städte von erheblicher Bedeutung sein, ohne bislang erfasst zu werden. Gleiches gilt für Einrichtungen von KRITIS-Betreibern, die eine zentrale Rolle bei der Aufrechterhaltung der IT-Sicherheit und der Abwehr von Cyberangriffen spielen.

- **Transparente Zwischenschritte im Verfahren schaffen:** Unternehmen sollten während des Aufnahme- und Überprüfungsverfahrens digital nachvollziehen können, welche Verfahrensschritte bereits abgeschlossen sind, welche vorbereitenden Maßnahmen sie bereits ergreifen können und wann mit einem Abschluss der Prüfung zu rechnen ist. Dadurch könnten Unternehmen früher an Produkten und Lösungen arbeiten und sich gezielter auf spätere Vertragsbeziehungen in diesem Bereich vorbereiten. Es sollte sichergestellt werden, dass dadurch keine zusätzlichen bürokratischen Hürden entstehen.

2. Verfahren harmonisieren

- **Sicherheitsüberprüfungen an Personen statt an Beschäftigungsverhältnisse binden:** Alle Personen, die über eine gültige Sicherheitsüberprüfung verfügen, sollten jederzeit und in jedem Beschäftigungskontext gemäß ihrem Einstufungsniveau eingesetzt werden können. Sicherheitsüberprüfungen sollten daher an Personen gebunden werden und nicht an Organisationen beziehungsweise Beschäftigungsverhältnisse. Orientierung bieten hierbei Modelle aus anderen europäischen Staaten, etwa aus dem Vereinigten Königreich und in begrenzter Form auch aus den Niederlanden. Dort bestehen Ansätze, bestehende Sicherheitsüberprüfungen beziehungsweise vergleichbare Nachweise unter bestimmten Voraussetzungen bei Wechseln zwischen Funktionen, Arbeitgebern oder Einsatzkontexten weiter nutzbar zu machen. Beispielsweise sollte ein ehemaliger Soldat oder Reservist, der über eine gültige Sicherheitsüberprüfung verfügt, diese nach dem Ausscheiden aus dem aktiven Dienstverhältnis auch für eine Tätigkeit in der Industrie nutzen können.

- **Behördenübergreifende Anerkennung von Sicherheitsüberprüfungen stärken:** Das SÜG sieht bereits vor, dass auf eine erneute Sicherheitsüberprüfung verzichtet werden kann, wenn innerhalb der letzten fünf Jahre eine gleich oder höherwertige Überprüfung ohne Feststellung eines Sicherheitsrisikos abgeschlossen wurde (§ 2 Abs. 1a Satz 1 Nr. 1 SÜG). Zudem kann die Sicherheitsakte zum Zweck dieser Prüfung der anfordernden Stelle zur Einsichtnahme übersandt werden (§ 18 Abs. 3 SÜG). Diese Kann-Regelungen sollten zu einer verbindlichen Anerkennung bereits erfolgter Sicherheitsüberprüfungen weiterentwickelt werden. Gleich- oder höherwertige Sicherheitsüberprüfungen sollten behördenübergreifend sowie bund-

und länderübergreifend grundsätzlich anerkannt werden. Eine erneute Überprüfung sollte nur in begründeten Ausnahmefällen erfolgen. Hierfür sollte die Verwaltung geeignete Nachweis- und Abfrageverfahren etablieren, damit eine gegenseitige Anerkennung rechtssicher und zweifelsfrei möglich wird.

- **Zentrale Betreuung von Unternehmen mit mehreren Bedarfsträgern:** Sofern Unternehmen für mehrere Bundes- oder Landesbehörden tätig werden, sollte eine federführende Stelle benannt werden, die die Geheimschutzbetreuung koordiniert. Dadurch können Doppelstrukturen reduziert, Verfahren vereinheitlicht und der Verwaltungsaufwand für Unternehmen sowie Behörden verringert werden. Ähnlich wie die Bundesagentur für Arbeit eine Ansprechstelle für Unternehmen hat, muss es auch im Bereich Geheimschutz eine zentrale Anlaufstelle geben – eine »Agentur für Trusted Vendoren« oder eine »Kompetenzstelle Sicherheit in der Wirtschaft«. Eine solche Stelle sollte zugleich dazu beitragen, Geheimschutzanforderungen ganzheitlicher zu betrachten und die Vorgaben aus dem Geheimschutzhandbuch und der Verschlusssachenanweisung stärker miteinander zu verzahnen.

- **Sabotageschutz, Geheimschutz und Zuverlässigkeitsüberprüfungen zusammendenken:** Bund, Länder und die zuständigen Behörden sollten einheitliche Standards und Zuständigkeiten für die Umsetzung sicherheitsbezogener Überprüfungen sicherstellen. Der Sabotageschutz ist dabei als gleichwertiger Bestandteil des Schutzkonzepts neben dem Geheimschutz zu betrachten. Zugleich sollten angrenzende Verfahren, etwa Zuverlässigkeitsüberprüfungen nach dem Luftsicherheitsgesetz, mitberücksichtigt werden, um Doppelstrukturen, uneinheitliche Maßstäbe und zusätzlichen Aufwand für Unternehmen zu vermeiden.

3. Effizienz stärken

- **Verfahren medienbruchfrei digitalisieren und beschleunigen:** Die Verfahren zur Aufnahme in die Geheimschutzbetreuung sowie die damit verbundenen Sicherheitsüberprüfungen sollten umfassend und medienbruchfrei digitalisiert werden. Ziel muss es sein, alle relevanten Verfahrensschritte digital abzubilden, Schnittstellen zwischen den beteiligten Stellen zu vereinheitlichen und Bearbeitungszeiten deutlich zu verkürzen. Ergänzend braucht es ausreichende personelle Ressourcen im BMWE und bei den beteiligten Sicherheitsbehörden sowie einheitliche Bewertungsmaßstäbe. KI-Anwendungen sollten dabei unterstützend eingesetzt werden und den Vorgaben der EU-KI-Verordnung sowie des Datenschutzrechts entsprechen.

- **Streichung des Verbots paralleler Tätigkeiten bei VS-Aufträgen:** Unternehmen sollten geprüfte Personen flexibler in VS-Aufträgen einsetzen können, auch wenn diese nicht unmittelbar bei dem eingesetzten Unternehmen angestellt sind. Das ist insbesondere relevant, wenn Spezialwissen projektbezogen benötigt wird, Beschäftigte innerhalb eines Konzerns eingesetzt werden sollen oder Unternehmen im Rahmen von Kooperationen zusammenarbeiten. Ein praktisches Beispiel sind matrixförmige Konzernstrukturen, etwa konzerninterne IT-Service-Gesellschaften, deren Beschäftigte in VS-Aufträgen anderer Konzernunternehmen eingesetzt werden sollen.

  Die bisherigen Vorgaben zum Einsatz von Fremdpersonal und zu Tätigkeiten für mehrere Unternehmen sollten daher praxistauglicher gestaltet werden. Pauschale

Beschränkungen können dazu führen, dass vorhandene Expertise nicht oder nur mit erheblichem zusätzlichem Aufwand genutzt werden kann. Entscheidend sollte künftig sein, dass der Einsatz geprüfter Personen grundsätzlich ermöglicht wird. Einschränkungen sollten nur greifen, wenn im konkreten Einsatz Sicherheitsrisiken, Interessenkonflikte oder unzulässige Zugriffe auf Verschlusssachen bestehen.

Deutschlands Verteidigungsfähigkeit hängt auch von schneller Lieferfähigkeit und einer anpassungsfähigen Sicherheits- und Verteidigungswirtschaft ab. Gerade in Zeiten schneller Innovationszyklen darf der Zugang zum Markt nicht durch langwierige und starre Sicherheitsüberprüfungen ausgebremst werden. Dafür braucht es einen praxistauglichen und zugleich sicheren Geheimschutz. Die erst kürzlich erfolgte Novellierung war ein wichtiger Schritt. Nun muss auch die praktische Ausgestaltung der Verfahren stärker an den aktuellen Bedürfnissen von Wirtschaft und sicherheitsrelevanter Innovation ausgerichtet werden.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Felix Kuhlenkamp | Leiter Sicherheit
T +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Nemo Buschmann | Referent Verteidigung & Öffentliche Sicherheit
T +49 30 27576-101 | n.buschmann@bitkom.org

Benjamin Spindeldreier | Junior Manager DefTech & Sicherheit
T +49 30 27576-379 | b.spindeldreier@bitkom.org

Verantwortliches Bitkom-Gremium
AK Verteidigung
AK Sicherheitspolitik
DefTech Network