



VSW-Positionspapier

Ein wichtiger Schritt zur Erhöhung der Resilienz Deutschlands

Zur Novelle des Sicherheitsüberprüfungsrechts

Das Wichtigste in Kürze

1. Sicherheitsempfindliche Stellen klar und risikobasiert definieren
2. Bereits durchgeführte Sicherheitsüberprüfungen anerkennen
3. Internationale Belegschaften angemessen berücksichtigen
4. Betriebs- und Geschäftsgeheimnisse wirksam schützen
5. Zuständigkeiten der Behörden transparent und einheitlich gestalten
6. Ausreichende Übergangsfristen und behördliche Kapazitäten sicherstellen
7. Staat und Wirtschaft frühzeitig und strukturiert einbinden
8. Sicherheitsüberprüfungsrecht mit KRITIS-, NIS2- und Cybersecurity-Anforderungen verzahnen

Anforderungen für Unternehmen müssen klar, verhältnismäßig und praktikabel sein

Der VSW-Bundesverband begrüßt die grundsätzliche Stoßrichtung der Novelle ausdrücklich. Insbesondere die stärkere Berücksichtigung hybrider Bedrohungen, von Sabotagerisiken und des Innentäterrisikos trägt der veränderten Sicherheitslage Rechnung.

Damit die vorgesehenen Regelungen in der Praxis wirksam umgesetzt werden können, sollten aus Sicht des VSW-Bundesverbands jedoch einige Punkte weiter konkretisiert und gestärkt werden. Entscheidend ist dabei ein risikobasierter und verhältnismäßiger Ansatz, der den Schutzbedarf berücksichtigt und zugleich für die betroffenen Unternehmen rechtssicher und praktikabel bleibt.

1. Sicherheitsempfindliche Stellen klar und risikobasiert definieren

Für Unternehmen muss eindeutig erkennbar sein, welche Funktionen und Stellen als sicherheitsempfindlich einzustufen sind. Eine konkretere und möglichst einheitliche Definition würde die Rechtssicherheit erhöhen und eine konsistente Anwendung durch die zuständigen Behörden unterstützen.

Sicherheitsüberprüfungen sollten sich dabei an der tatsächlichen Kritikalität einer Funktion und dem damit verbundenen Risiko orientieren. Nicht jede Tätigkeit innerhalb eines betroffenen Unternehmens weist das gleiche Gefährdungspotenzial auf. Ein risikobasierter Ansatz ermöglicht es, Sicherheitsmaßnahmen gezielt dort einzusetzen, wo sie tatsächlich erforderlich sind. Zugleich stärkt er die Akzeptanz der Regelungen und vermeidet unnötige Belastungen für Unternehmen und Beschäftigte.

2. Bereits durchgeführte Sicherheitsüberprüfungen anerkennen

Doppel- und Mehrfachüberprüfungen sollten vermieden werden. Bereits durchgeführte Sicherheitsüberprüfungen sollten daher behörden- und betreiberübergreifend anerkannt werden können, sofern Überprüfungsart, Umfang und Sicherheitsniveau vergleichbar sind.

Dies ist insbesondere für Unternehmen mit komplexen oder internationalen Strukturen von Bedeutung. Für große digitale Infrastrukturanbieter und Hyperscaler sollte zudem die

Möglichkeit geschaffen werden, Beschäftigte nach einem einheitlich definierten Sicherheitsstandard überprüfen zu lassen, der anschließend von den jeweils zuständigen Stellen anerkannt wird.

Ein vergleichbarer Ansatz sollte auch für die Sicherheit von Rechenzentren und anderen besonders schutzbedürftigen Infrastrukturen gelten.

3. Internationale Belegschaften angemessen berücksichtigen

Viele Unternehmen arbeiten heute mit internationalen Teams und grenzüberschreitenden Projektstrukturen. Für Beschäftigte mit ausländischer Staatsangehörigkeit oder relevanten Aufenthalt- und Beschäftigungszeiten im Ausland müssen deshalb praktikable und rechtssichere Verfahren für Sicherheitsüberprüfungen vorgesehen werden.

Dies ist nicht zuletzt vor dem Hintergrund des zunehmenden Fachkräftemangels von Bedeutung. Verfahren müssen einerseits den erforderlichen Sicherheitsstandard gewährleisten, andererseits aber auch die tatsächlichen Möglichkeiten der Unternehmen und der zuständigen Behörden berücksichtigen.

4. Betriebs- und Geschäftsgeheimnisse wirksam schützen

Bei Sicherheitsüberprüfungen können Informationen über Unternehmen, Geschäftsmodelle, technologische Entwicklungen oder interne Strukturen berührt werden. Deshalb sollte eindeutig geregelt werden, welche Informationen erhoben, verarbeitet und an welche Stellen übermittelt werden dürfen.

Der Schutz von Betriebs- und Geschäftsgeheimnissen, sensiblem Know-how und geistigem Eigentum muss dabei angemessen berücksichtigt werden. Sicherheitsüberprüfungen dürfen nicht dazu führen, dass schutzwürdige Unternehmensinformationen über das für die Durchführung der Überprüfung erforderliche Maß hinaus offengelegt werden.

5. Zuständigkeiten der Behörden transparent und einheitlich gestalten

Für Unternehmen muss eindeutig erkennbar sein, welche Behörde für welchen Prozess und welche Beschäftigtengruppe zuständig ist. Der VSW-Bundesverband spricht sich daher für transparente und bundesweit möglichst einheitliche Zuständigkeitsstrukturen aus.

Gerade bei bundesweit oder international tätigen Unternehmen sind unterschiedliche Verfahren und Zuständigkeiten mit erheblichem organisatorischem Aufwand verbunden. Einheitliche Ansprechpartner und standardisierte Prozesse könnten die Umsetzung deutlich erleichtern und zugleich die Bearbeitung auf Seiten der Behörden effizienter gestalten.

6. Ausreichende Übergangsfristen und behördliche Kapazitäten sicherstellen

Die Umsetzung neuer Sicherheitsüberprüfungen erfordert auf Seiten der Unternehmen erhebliche organisatorische Vorbereitungen. Gleichzeitig müssen die zuständigen Behörden in der Lage sein, die zusätzlich entstehenden Verfahren innerhalb angemessener Fristen zu bearbeiten.

Deshalb sind ausreichende Übergangsfristen, ausreichende behördliche Bearbeitungskapazitäten und geeignete Priorisierungsmechanismen erforderlich.

Für bereits eingesetztes Personal sollte zudem eine angemessene Bestandsschutz- beziehungsweise Übergangsregelung vorgesehen werden. Unternehmen benötigen Planungssicherheit, damit der Betrieb kritischer und sicherheitsrelevanter Infrastrukturen nicht durch langwierige Überprüfungsverfahren beeinträchtigt wird.

7. Staat und Wirtschaft frühzeitig und strukturiert einbinden

Die Betreiber kritischer und verteidigungsrelevanter Infrastrukturen verfügen über umfangreiche praktische Erfahrungen im Umgang mit Sicherheitsrisiken. Dieses Wissen sollte stärker für die Ausgestaltung und Weiterentwicklung der Regelungen genutzt werden.

Der VSW-Bundesverband hält deshalb eine frühzeitige und strukturierte Einbindung der Wirtschaft insbesondere bei der Identifikation neuer sicherheitsempfindlicher Bereiche und Funktionen für sinnvoll. Regelmäßiger Austausch zwischen Staat, Sicherheitsbehörden und Unternehmen kann dazu beitragen, Anforderungen praxistauglich auszugestalten und neue Gefährdungslagen schneller zu berücksichtigen.

8. Sicherheitsüberprüfungsrecht mit KRITIS-, NIS2- und Cybersecurity-Anforderungen verzahnen

Die Novelle sollte stärker mit den bereits bestehenden und parallel entstehenden Regelungen zum Schutz kritischer Infrastrukturen und zur Cybersicherheit verzahnt werden. Dies gilt insbesondere für die KRITIS- und NIS2-Regulierung sowie für Anforderungen an den Schutz sensibler Unternehmensinformationen und der digitalen Infrastruktur.

Unternehmen benötigen ein möglichst konsistentes und aufeinander abgestimmtes Sicherheitsregime, statt parallel bestehender Anforderungen mit unterschiedlichen Definitionen, Zuständigkeiten und Nachweispflichten.

In diesem Zusammenhang sollte auch geprüft werden, ob die wiederkehrende Verwendung des Begriffs „lebenswichtig“ durch den Begriff „existentiell“ beziehungsweise „existenzielle Bereiche“ präzisiert werden kann. Entscheidend ist, dass die verwendeten Begriffe eindeutig, rechtssicher und mit den entsprechenden Regelungen anderer Sicherheits- und Resilienzbereiche kompatibel sind.

Fazit

Die Novelle ist ein wichtiger Schritt, um Deutschland besser gegen hybride Bedrohungen, Sabotage und Innentäters Risiken zu schützen. Ihre Wirksamkeit wird jedoch maßgeblich davon abhängen, ob die neuen Anforderungen in der Praxis umsetzbar sind.

Aus Sicht des VSW-Bundesverbands müssen die Regelungen deshalb klar, risikobasiert, verhältnismäßig und praktikabel ausgestaltet werden. Unternehmen benötigen eindeutige Kriterien, verlässliche Zuständigkeiten und angemessene Übergangsfristen. Gleichzeitig müssen Sicherheitsüberprüfungen effizient durchgeführt und bereits vorhandene Sicherheitsstandards soweit möglich anerkannt werden.

Ein wirksamer Wirtschaftsschutz entsteht dort, wo Staat, Sicherheitsbehörden und Wirtschaft ihre jeweiligen Kompetenzen zusammenführen. Eine frühzeitige und kontinuierliche Zusammenarbeit ist daher ein zentraler Erfolgsfaktor für eine praxistaugliche und zukunftsfähige Ausgestaltung des Sicherheitsüberprüfungsrechts.