bitkom

# Stellungnahme

September 2026

# Neufassung und Änderung der Sicherheitsüberprüfungsfeststellungs-verordnung (SÜFV)

## Zusammenfassung

Bitkom begrüßt grundsätzlich das Ziel des Referentenentwurfs, den vorbeugenden personellen Sabotageschutz angesichts der veränderten Sicherheitslage zu stärken. Die Ausweitung des Anwendungsbereichs auf weitere sicherheitsrelevante Bereiche ist folgerichtig. Der Referentenentwurf selbst begründet die Novelle mit der gestiegenen Bedrohung durch hybride Angriffe und Sabotagehandlungen durch sogenannte Innentäter und sieht deshalb die Aufnahme weiterer Wirtschaftszweige und Anwendungsfälle vor.

Mit der Ausweitung des Anwendungsbereichs wird zugleich die Zahl der Unternehmen und Beschäftigten steigen, die Sicherheitsüberprüfungsverfahren durchlaufen müssen. Damit die neuen Regelungen ihre Schutzwirkung in der Praxis entfalten können, müssen die Verfahren deshalb einfacher, digitaler und schneller werden, ohne das bestehende Sicherheitsniveau abzusenken. Administrative Prozesse sollten konsequent digitalisiert und bestehende Verfahren beschleunigt werden. Zugleich sollte die SÜFV die tatsächliche Kritikalität von Einrichtungen stärker berücksichtigen und Mehrfachüberprüfungen aufgrund unterschiedlicher Regelungen von Bund und Ländern vermeiden. Ein wirksamer personeller Sabotageschutz setzt voraus, dass Sicherheitsüberprüfungen nicht nur hohen Sicherheitsanforderungen genügen, sondern auch effizient und für Unternehmen handhabbar ausgestaltet sind.

Die notwendige Modernisierung darf sich dabei nicht auf die Verfahren der Sicherheitsüberprüfung beschränken. Auch die Vorgaben des Geheimschutzhandbuchs sollten stärker an heutigen technologischen Entwicklungen und modernen Sicherheitsarchitekturen ausgerichtet werden. Ansätze wie Zero Trust, aktuelle Verschlüsselungsstandards und zeitgemäße Endgerätekonzepte müssen angemessen berücksichtigt werden. Ziel sollte ein Regelungsrahmen sein, der hohe Anforderungen

an den Geheimschutz mit modernen technischen Schutzmechanismen verbindet und Unternehmen eine sichere und zugleich zeitgemäße Umsetzung ermöglicht.

## Begrüßenswerte Ausweitung des Anwendungsbereichs

Die grundsätzliche Stoßrichtung der Neufassung ist aus Sicht des Bitkom richtig. Angesichts der verschärften Sicherheitslage ist es notwendig, den vorbeugenden personellen Sabotageschutz weiterzuentwickeln und bislang nicht oder nicht ausreichend erfasste kritische Bereiche einzubeziehen. Dies betrifft unter anderem die Bereiche Energie, Wasser, IT-Sicherheitsprodukte, Telekommunikationsanlagen und Rechenzentren. Der Referentenentwurf erweitert den Kreis der erfassten lebenswichtigen Einrichtungen entsprechend.

Entscheidend ist jedoch, dass der Anwendungsbereich die tatsächliche Kritikalität der jeweiligen Einrichtungen angemessen erfasst und die mit der Ausweitung verbundenen Sicherheitsüberprüfungen für Unternehmen praktisch umsetzbar bleiben.

## § 16 SÜFV: Mehrfachüberprüfungen vermeiden

Nach der in § 16 vorgesehenen Öffnungsklausel findet der betreffende Abschnitt der SÜFV auf Wasserwerke in öffentlicher Trägerschaft und Rechenzentren keine Anwendung, soweit diese zumindest auch staatliche Aufgaben auf Landesebene wahrnehmen. Weitergehende landesrechtliche Regelungen bleiben ausdrücklich unberührt.

Dem Ziel, den Ländern zusätzlichen Handlungsspielraum einzuräumen, steht grundsätzlich nichts entgegen. Gleichzeitig besteht jedoch die Gefahr, dass Unternehmen, die Leistungen für mehrere Länder erbringen, mit unterschiedlichen landesrechtlichen Sicherheitsüberprüfungen konfrontiert werden. Beschäftigte könnten dadurch für vergleichbare Tätigkeiten mehrfach überprüft werden, ohne dass damit ein entsprechender zusätzlicher Sicherheitsgewinn verbunden wäre.

Unklar ist zudem, wie mit Beschäftigten umzugehen ist, die bereits für eine sicherheitsempfindliche Tätigkeit überprüft wurden und anschließend in einem anderen sicherheitsempfindlichen Bereich eingesetzt werden sollen. Auch in diesen Fällen muss vermieden werden, dass bereits erfolgte Sicherheitsüberprüfungen ohne sachlichen Grund erneut durchgeführt werden müssen.

Bitkom spricht sich daher für eine bundesweit möglichst einheitliche Handhabung der Sicherheitsüberprüfungen durch die Länder aus. Zumindest muss sichergestellt werden, dass gleichwertige Sicherheitsüberprüfungen anderer Länder sowie, soweit sachgerecht, bereits auf Bundesebene durchgeführte Überprüfungen gegenseitig anerkannt werden. Mehrfachüberprüfungen derselben Personen müssen vermieden werden.

## § 20 SÜFV: Leitstellen großer Elektrizitätsverteilernetze einbeziehen

Der Referentenentwurf sieht in § 20 Absatz 1 Nummer 3 vor, Leitstellen für Elektrizitätsverteilernetze als lebenswichtige Einrichtungen zu erfassen, wenn deren maximale Entnahme- oder Rückspeiseleistung aus dem Elektrizitätsübertragungsnetz im jeweils vorangegangenen Kalenderjahr über 584 Megawatt betragen hat.

Dieser Schwellenwert ist aus unserer Sicht zu hoch angesetzt. Dadurch können Leitstellen großer Elektrizitätsverteilernetze außerhalb des Anwendungsbereichs bleiben, obwohl sie für die Versorgung großer urbaner Räume von erheblicher Bedeutung sind.

Bitkom spricht sich daher dafür aus, § 20 Absatz 1 Nummer 3 um ein weiteres Kriterium zu ergänzen. Erfasst werden sollten auch Leitstellen für Elektrizitätsverteilernetze, die mehr als 500.000 zu versorgende Einwohnerinnen und Einwohner umfassen. Der Schwellenwert von 500.000 Einwohnern entspricht dem Kritikalitätsschwellenwert des KRITIS-Dachgesetzes und trägt zugleich zu einer stärkeren Kohärenz zwischen thematisch eng miteinander verbundenen Regelungen bei.

**Änderungsvorschlag zu § 20 Absatz 1 Nummer 3 SÜFV:** »Leitstellen für Elektrizitätsverteilernetze betreiben, deren maximale Entnahme- oder Rückspeiseleistung aus dem Elektrizitätsübertragungsnetz im jeweils vorangegangenen Kalenderjahr über 584 Megawatt betragen hat, oder die mehr als 500.000 zu versorgende Einwohnerinnen und Einwohner umfassen.«

## § 20 Absatz 2 Satz 1 Nummer 2 SÜFV: Anwendungsbereich für Mobilfunkunternehmen klarstellen

Unklar ist, ob Mobilfunkunternehmen, die nach § 164a TKG öffentliche Warnungen mittels Cell Broadcast verbreiten, von § 20 Absatz 2 Satz 1 Nummer 2 SÜFV-E erfasst werden. Die Verpflichtung zur Warnungsverbreitung beruht dabei nicht auf § 6 des Zivilschutz- und Katastrophenhilfegesetzes (ZSKG) oder einer öffentlich-rechtlichen Beauftragung, sondern unmittelbar auf den Vorgaben des TKG und den hierzu erlassenen technischen Regelungen. Bitkom bittet daher um Klarstellung, ob Mobilfunkunternehmen beziehungsweise die mit Cell Broadcast befassten Unternehmensteile in den Anwendungsbereich der Vorschrift fallen sollen. Sollte dies beabsichtigt sein, sollte zugleich geprüft werden, ob die Einbeziehung der ausschließlich technisch mit der Verbreitung von Warnmeldungen befassten

Beschäftigten in den vorbeugenden personellen Sabotageschutz sachgerecht und verhältnismäßig ist.

## § 20 SÜFV: Zentrale IT-Sicherheitsfunktionen von KRITIS-Betreibern erfassen

Die IT-Sicherheit ist für den sicheren Betrieb kritischer Infrastrukturen von zentraler Bedeutung. Bislang werden Einrichtungen von KRITIS-Betreibern, die für die Aufrechterhaltung der IT-Sicherheit sowie für die Erkennung und Abwehr von Cyberangriffen verantwortlich sind, jedoch nicht ausdrücklich als lebenswichtige Einrichtungen erfasst.

Damit bleibt Personal, das an entsprechenden sicherheitsrelevanten Stellen eingesetzt wird oder eingesetzt werden soll, außerhalb des vorgesehenen Anwendungsbereichs. Aus Sicht des Bitkom sollte diese Lücke geschlossen werden.

Wir schlagen daher vor, § 20 Absatz 1 SÜFV um eine neue Nummer 8 zu ergänzen.

**Ergänzungsvorschlag zu § 20 Absatz 1 SÜFV:** »8. die als Betreiber kritischer Infrastrukturen Einrichtungen betreiben, welche für die Aufrechterhaltung der IT-Sicherheit oder die Erkennung und Abwehr von Cyberangriffen von zentraler Bedeutung sind.«

## Ausreichende Übergangsfrist für neu erfasste Unternehmen

Die Ausweitung des Anwendungsbereichs führt dazu, dass Unternehmen und Unternehmensteile erstmals den Anforderungen des vorbeugenden personellen Sabotageschutzes unterliegen und entsprechende Sicherheitsüberprüfungen für Beschäftigte veranlassen müssen.

Die bestehende Jahresfrist nach § 25a SÜG kann sich dabei insbesondere dann als zu knapp erweisen, wenn Beschäftigte aufgrund ihrer persönlichen Voraussetzungen – etwa aufgrund einer ausländischen Staatsangehörigkeit oder eines noch nicht ausreichend langen Aufenthalts in Deutschland – nicht oder nicht rechtzeitig überprüft werden können.

Unternehmen benötigen in diesen Fällen ausreichend Zeit, ihre Personal- und Organisationsstrukturen an die neuen Anforderungen anzupassen, ohne den laufenden Betrieb zu gefährden. Bitkom regt daher an, für erstmals von der SÜFV erfasste Unternehmen und Unternehmensteile eine längere beziehungsweise angemessen flexible Übergangsregelung vorzusehen.

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

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



## Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik
AK Öffentliche Sicherheit
AK Verteidigung