



KRITIS-Dachgesetz und BSIG als neue Säulen der Unternehmensresilienz.

Im März 2026 ist das KRITIS-Dachgesetz in Kraft getreten. Es setzt die Europäische Resilienz-Richtlinie um und verpflichtet die betroffenen Unternehmen zu physischen Sicherheitsmaßnahmen. Es stellt das Pendant zum BSIG dar, das die IT-Sicherheit adressiert und seit Ende 2025 die NIS-2-Richtlinie umsetzt. Die Gesetze sollen „Hand in Hand greifen“, damit Unternehmen in einer hybriden Sicherheitslage resilient aufgestellt sind. Typische Anwendungsfälle des neuen Gesetzes sind Naturereignisse, Sabotagehandlungen, Drohnensichtungen, Lieferkettenausfälle sowie umfassende Engpässe bei Personalressourcen, wie sie in pandemischen Lagen entstehen können.

Während die Umsetzung der NIS-2-Richtlinie viel Aufmerksamkeit bei den Unternehmen erlangt hat, hinkt das KRITIS-Dachgesetz hier oft noch hinterher. In unserem SR.-Whitepaper zeigen wir Ihnen, wie Sie eine effektive und ressourcenschonende Umsetzung des Gesetzes angehen können.

Anwendungsbereich von KRITIS-Dachgesetz und BSIG im Chemie- und Pharmasektor.

Vor dem Hintergrund des oben beschriebenen All-Gefahren-Ansatzes gibt es gewisse Schnittmengen bei den Betreiberkategorien in den Anwendungsbereichen von KRITIS-Dachgesetz und BSIG.

Der Anwendungsbereich des BSIG ist deutlich größer als der des KRITIS-Dachgesetzes. Denn das BSIG kennt die Kategorien der **wichtigen Einrichtungen** (wE) und **besonders wichtigen Einrichtungen** (bwE). Sie zeichnen sich dadurch aus, dass sie über eine bestimmte Unternehmensgröße verfügen (ab 50 Mitarbeitenden oder ein Jahresumsatz und eine Jahresbilanzsumme von 10 Mio. EUR) und einer Tätigkeit aus den Anlagen 1 und 2 des BSIG nachgehen. Folgende Tätigkeiten sind hier für die Chemie- und Pharmabranche relevant, wobei in Einzelfällen auch weitere Tätigkeiten hinzukommen können (bspw. Stromerzeugung mit Einspeisung in das öffentliche Netz):

BSIG – Anlage 1 (differenziert zwischen wE und bwE)
Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach § 2 AMG ausüben
Unternehmen, die pharmazeutische Erzeugnisse nach Abschnitt C Abt. 21 NACE Rev. 2 herstellen
Hersteller von Medizinprodukten, die auf der „Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“ geführt werden
Managed Services Provider (auch interne Konzern-IT)
BSIG – Anlage 2 (erfasst alle Unternehmen als wE)
Hersteller und Importeure nach Art. 3 Nr. 9 und Nr. 11 REACH-VO von chemischen Stoffen und Gemischen (Art. 3 Nr. 1, Nr. 2 REACH-VO), sofern sie in Kategorie 20 NACE Rev. 2 fallen und nach Art. 6 REACH-VO registrierungspflichtig sind



Unternehmen müssen das KRITIS-Dachgesetz nicht isoliert betrachten. Entscheidend ist, bestehende Security-Strukturen sinnvoll zusammenzuführen und gezielt weiterzuentwickeln.

Dr. Kim Manuel Künstner, Rechtsanwalt, Partner | Data, Digital & Governance
Berät Unternehmen zu Cybersecurity, KI-Regulierung und Compliance

Hinzu kommt die Einrichtungskategorie der **Betreiber kritischer Anlagen**. Im BSIG stellt das eine Sonderform der bwE dar, im Kritis-Dachgesetz ist es die einzige Einrichtungskategorie. In diesem Punkt findet also die Schnittmenge statt. Wer Betreiber einer kritischen Anlage ist, wird über eine Rechtsverordnung bestimmt, die künftig auf das KRITIS-Dachgesetz gestützt wird. Die Kritis-Verordnung befindet sich im Entwurfsstadium und wird die BSI-Kritisverordnung ablösen. Diese Verordnung bestimmt für die einschlägigen Sektoren Schwellenwerte, ab denen eine Anlage als erheblich anzusehen ist und erfasst ist. Zu den Anlagen werden im Chemie- und Pharmabereich zählen:

Anlagenart in KritisV	Schwellenwert
Versorgung mit lebenserhaltenden, zur Verhinderung schwerer gesundheitlicher Folgen oder zur Bewältigung von Notlagen im Bereich der öffentlichen Gesundheit erforderlichen Medizinprodukten	
Produktionsstätte	Jahresumsatz > 90,68 Mio. EUR
Abgabestelle nach Medizinprodukte-Abgabeverordnung	Jahresumsatz > 90,68 Mio. EUR
Versorgung mit versorgungsrelevanten Wirkstoffen und daraus herzustellenden Arzneimitteln, Impfstoffen und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper	
Produktionsstätte zur Herstellung versorgungsrelevanter Wirkstoffe und daraus herzustellender Arzneimittel	4,65 Mio. in Verkehr gebrachte Packungen verschreibungspflichtiger Arzneimittel/Jahr
Produktionsstätte zur Herstellung von pharmazeutischen Grundstoffen (u.a. aktive pharmazeutische Inhaltsstoffe, chemisch reiner Zucker)	Noch unklar
Vertriebsweg für Arzneimittel	4,65 Mio. umgeschlagene Arzneimittel verschreibungspflichtiger Packungen/Jahr
Blut- und Plasmaspendensteuerungssystem	34.000 hergestellte oder in Verkehr gebrachte Produkte/Jahr
Abgabe in Apotheken	4,65 Mio. abgegebene Packungen verschreibungspflichtiger Arzneimittel/Jahr
Erforschung und Entwicklung von potentiell versorgungsrelevanten Wirkstoffen und daraus herzustellenden Arzneimitteln zur Anwendung im oder am menschlichen Körper	
Anlage zur Entwicklung [und Herstellung] von für die weitere Forschung bestimmten Arzneimitteln	61,36 Mio. EUR Investitionen in Forschung & Entwicklung/Jahr

Während es für die wE und bwE Zurechnungsvorschriften von Verbundsunternehmen gibt und Nebentätigkeiten außer Acht gelassen werden dürfen, gibt es in der Kritis-Verordnung je nach Anlage spezielle Zurechnungsvorschriften, wann von einer gemeinsamen Anlage auszugehen ist und welche Nebeneinrichtungen bei einer Anlage hinzuzurechnen sind. Die Anwendbarkeit von BSIG und KRITIS-DachG werden mittels einer **Betroffenheitsprüfung** bestimmt. Zudem können Unternehmen mittelbar betroffen sein, wenn Betreiber Sicherheitsvorgaben innerhalb der Lieferkette weitergeben.



Wer sich frühzeitig mit den neuen Anforderungen auseinandersetzt, reduziert nicht nur regulatorische Risiken, sondern stärkt zugleich die Widerstandsfähigkeit seines Unternehmens.

Thorsten Walter, Rechtsanwalt, Partner | Data, Digital & Governance

Berät Unternehmen zu Cybersecurity, KI-Regulierung und Compliance

Überblick zu den Rechtsfolgen des Kritis-Dachgesetzes.

Wer in den Anwendungsbereich fällt, muss sich als Betreiber registrieren. Die **Registrierungspflicht** gilt frühestens ab dem 17. Juli 2026 und ist noch abhängig von einer Konkretisierung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK), das die Aufsichtsbehörde zum KRITIS-Dachgesetz ist. Die Registrierung wird über das Registrierungsportal von BBK und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) stattfinden. Laut BBK muss eine Registrierung erst erfolgen, wenn die Kritis-Verordnung erlassen ist.

Im Kern steht dann die Einrichtung von Resilienzmaßnahmen, um dafür zu sorgen, dass die Anlage präventiv vor physischen Ereignissen mit Betriebsbeeinträchtigungsrisiken geschützt ist und gleichzeitig auf niemals gänzlich zu vermeidende Vorfälle eingestellt ist. Beispielhaft zu nennen sind dann etwa Zugangskontrollen, Videoüberwachung, Abläufe im Alarmfall sowie die Sicherheit in der Lieferkette. Die Resilienzmaßnahmen werden in einem **Resilienzplan** festgehalten. Sie können durch das BBK geprüft werden, es kann

auch Nachweise zur Umsetzung der Vorgaben verlangen. Das geschieht praktisch über Audits.

Welches Maß gilt für Resilienzmaßnahmen?

Grundlage sämtlicher Resilienzmaßnahmen ist eine dokumentierte **Risikoanalyse und -bewertung**. Betreiber müssen ihre Risiken regelmäßig identifizieren, bewerten und priorisieren. Dabei sind insbesondere die nationale Risikoanalyse sowie weitere vertrauenswürdige Informationsquellen einzubeziehen. Die Analyse ist mindestens alle vier Jahre zu aktualisieren. Leider wird die nationale Risikoanalyse und -bewertung noch einige Zeit auf sich warten lassen, bis dahin sind also andere Informationsquellen heranzuziehen. Das gilt etwa für Anfragen bei den örtlichen Umweltbehörden über Naturrisiken. Zudem können Störfallbetreiber die Ergebnisse einer durchgeführten Gefahren- und Risikoanalyse heranziehen.

Maßstab für die Resilienzmaßnahmen ist die **Angemessenheit**, der Stand der Technik soll eingehalten werden. Die Unternehmen vergleichen den Aufwand für den Schutz vor einem Vorfall mit den Folgen, sollte der Vorfall ohne Schutzmaßnahmen eintreten. Hilfreich werden Branchenspezifische Resilienzstandards sein, die Branchenverbände erstellen. Sie konkretisieren standardisierte Management-Prozesse und werden vom BBK für einen bestimmten Zeitraum als geeignet erklärt. Wer die Standards umsetzt und dies sorgfältig dokumentiert, für den gilt die Vermutung, dass er alles getan hat, was von ihm verlangt wird.

Meldepflicht von KRITIS-Dachgesetz und BSIG.

Beide Gesetze sehen bei erheblichen Sicherheitsvorfällen eine Meldepflicht an die **gemeinsame Meldestelle von BBK und BSI** vor. Leider sind beide Vorschriften nicht kongruent ausgestaltet, was etwa die Fristen für die Meldungen betrifft. Auf jeden Fall muss unverzüglich, spätestens innerhalb der ersten 24 Stunden nach Kenntnisnahme vom Vorfall eine Meldung abgegeben werden. Im BSIG erfolgt spätestens bis 72 Stunden nach Kenntnisnahme eine weitere Meldung, in beiden Gesetzen gibt es nach einem Monat eine Abschlussmeldung. Ist die Vorfallobarbeitung noch nicht abgeschlossen, müssen Aktualisierungsmeldungen erfolgen.

Ressourcenschonende Umsetzung des KRITIS-Dachgesetzes.

Sowohl das KRITIS-Dachgesetz als auch das BSIG verpflichten ausdrücklich die **Geschäftsleitung**, dass sie die Umsetzung der gesetzlichen Vorgaben mittels organisatorischer Prozesse überwachen muss. Missachtet sie die Pflicht zur Letztverantwortung, haftet sie für deshalb eintretende Schäden persönlich. Während im BSIG eine Schulungspflicht ausdrücklich vorgesehen ist, fehlt diese Regelung im KRITIS-Dachgesetz. Sie ist aber ohnehin die Grundvoraussetzung,

damit die Leitung mit ausreichender Sorgfalt ihrer Compliance-Verantwortung nachkommen kann.

Die gesetzlichen Vorgaben zur Unternehmenssicherheit steigen stetig an. Das zwingt Unternehmen dazu, Synergien zu finden und vorhandenes Knowhow in den Abteilungen zu nutzen. Daher muss eine „Inventur“ stattfinden, um Maßnahmen, Prozesse, Übungen, Richtlinien oder Fach- und Arbeitsgruppen ausfindig zu machen, die für die Umsetzung des KRITIS-Dachgesetzes in Frage kommen.

Die Ergebnisse müssen im Einzelfall bewertet werden, welche Zielrichtung sie verfolgen und welche **Risikoerwägungen** ihr zugrunde liegen. Je nach Einzelfall erfordert das KRITIS-Dachgesetz dann eine anderweitige Bewertung. Die Maßnahmen können aus folgenden Bereichen stammen:



Aus organisatorischer Sicht bietet sich aufgrund der stetig wachsenden Sicherheitspflichten die Etablierung einer Unternehmensfunktion ein, die die Risikomanagement-Prozesse lenkend abstimmt.



Unser Ziel ist nicht nur die rechtskonforme Umsetzung des KRITIS-Dachgesetzes, sondern die Entwicklung praktikabler Lösungen, die sich in bestehende Unternehmensprozesse integrieren lassen.

Dr. Tilmann Dittrich, Rechtsanwalt | Data, Digital & Governance
Berät Unternehmen zu Cybersecurity, KI-Regulierung und Compliance

Wobei helfen wir Ihnen?

1. Durchführung einer Betroffenheitsprüfung bzw. Ergänzung einer durchgeführten NIS-2-Betroffenheitsprüfung
2. Unterstützung bei der Umsetzungsstrategie für das KRITIS-Dachgesetz
3. Begleitung bei der „Inventur“ (Gap-Analyse) zu Risiken und bisher getroffenen Resilienzmaßnahmen
4. Ausformung gesetzlicher Risikomanagement-Maßnahmen nach dem KRITIS-Dachgesetz
5. Abstimmung von Meldeprozessen zwischen BSIG und KRITIS-Dachgesetz
6. Begleitung in behördlichen Aufsichtsverfahren zum KRITIS-Dachgesetz
7. Strukturiertes „Lessons Learned“ nach einem Sicherheitsvorfall
8. Ergänzung der NIS-2-Leitungsschulungen um die Basics des KRITIS-Dachgesetzes

Ihre Berater.



Dr. Kim Manuel Künstner
Rechtsanwalt, Partner.

kim.kuenstner@schulte-lawyers.com



Thorsten Walter
Rechtsanwalt, Partner.

thorsten.walter@schulte-lawyers.com



Dr. Tilmann Dittrich
Rechtsanwalt, Associate.

tilmann.dittrich@schulte-lawyers.com

SCHULTE RECHTSANWÄLTE. Rechtsanwaltsgesellschaft mbH

**Neue Mainzer Straße 28
60311 Frankfurt am Main
T: +49 69 900 26-6**

