# Wirtschaftsschutz unter neuen Vorzeichen

**Von Holger Köster**

**Holger Köster**

Geschäftsführer der HERSA-Unternehmensgruppe und Vorsitzender des Fachausschusses Wirtschaftsschutz im BDSW

Der Druck auf Unternehmen, Risiken systematischer zu erfassen und Schutzmaßnahmen besser zu verzahnen, nimmt durch neue Regulierungen und Gesetze spürbar zu. Ob aus diesen tatsächlich mehr Sicherheit entsteht, entscheidet sich jedoch in der praktischen Umsetzung.

Mit NIS2 und dem KRITIS-Dachgesetz haben die Anforderungen an den Schutz von Unternehmen und kritischen Infrastrukturen deutlich zugenommen. Was lange vor allem als unternehmerische Vorsorge verstanden wurde, ist inzwischen stärker gesetzlich geregelt und mit konkreten Pflichten verbunden. Doch es zeigt sich immer wieder, dass neue Vorschriften allein noch keinen wirksamen Schutz gewährleisten.

Der Drohnenvorfall Anfang August 2026 am Flughafen Leipzig/Halle hat uns das wieder deutlich vor Augen geführt. Denn eine mit Sprengstoff und einer Zündvorrichtung versehene Drohne an einem wichtigen Verkehrsknotenpunkt wirft Fragen auf, die weit über diesen einzelnen Fall hinausgehen. Wie gut sind Unternehmen auf bekannte Bedrohungen vorbereitet? Sind Zuständigkeiten und Meldewege geklärt? Und funktionieren die vorgesehenen Maßnahmen auch dann, wenn tatsächlich etwas passiert?

Mit dem KRITIS-Dachgesetz rückt die physische Resilienz stärker in den Blick, während NIS2 die Anforderungen an die Cybersicherheit erheblich ausgeweitet hat. Unternehmen müssen jetzt Risiken umfassender betrachten und Sicherheitsmaßnahmen stärker miteinander verzahnen. Physische Sicherheit, Informationssicherheit, Risikomanagement und Business Continuity Management können deshalb nicht weiter unabhängig voneinander behandelt werden.

Auch für unsere Branche ergeben sich daraus neue Anforderungen. Sicherheitsdienstleister kennen die Standorte und betrieblichen Abläufe ihrer Kunden meist sehr genau. Dieses Wissen kann weit über die Erfüllung eines einzelnen Bewachungsauftrags hinaus wertvoll sein, etwa bei der Risikoanalyse ebenso oder der Gestaltung funktionierender Melde- und Reaktionsprozesse.

Der Wirtschaftsschutz insgesamt wird anspruchsvoller. Dabei bietet sich privaten Sicherheitsdienstleistern die Möglichkeit, ihre Erfahrungen aus der täglichen Praxis stärker einzubringen. Denn am Ende müssen sich Sicherheitskonzepte dort bewähren, wo wir als Branche seit jeher tätig sind: im realen Betrieb unserer Kunden.

Ihr
Holger Köster

Bild: # 1297225530 / istockphoto.com

# Regulierung schafft noch keine Sicherheit

## Wie NIS2 und KRITIS-Dachgesetz Unternehmen stärker in die Verantwortung nehmen

**Von Andreas Albrecht**

Mit NIS2 und KRITIS-Dachgesetz steigen die Anforderungen an Unternehmen. Der Drohnenfund am Flughafen Leipzig/Halle zeigt zugleich, dass bekannte Sicherheitslücken damit nicht automatisch geschlossen sind. Für den Wirtschaftsschutz wächst die Aufgabe, regulatorische Vorgaben in wirksame Vorsorge zu übersetzen.

**Andreas Albrecht**

Freier Fachredakteur und Journalist

Am Flughafen Leipzig/Halle wurde Anfang August eine Drohne gefunden, an der sich Sprengstoff und eine Zündvorrichtung befanden. Spezialkräfte entschärften den Sprengsatz, die Bundesanwaltschaft übernahm die Ermittlungen. Wer hinter dem Vorfall steckt und welches konkrete Ziel verfolgt wurde, war zum Redaktionsschluss dieser Ausgabe (7. August 2026) zwar noch ungeklärt. Unabhängig von der Täterfrage kam dieser Vorfall für viele Sicherheitsexperten allerdings nicht völlig überraschend. Seit Jahren wird davor gewarnt, dass Drohnen kritische Infrastrukturen nicht nur ausspähen, sondern auch unmittelbar gefährden können. Manuel Atug, Gründer und Sprecher der unabhängigen AG KRITIS, bezeichnete beispielsweise in einer ersten Stellungnahme gegenüber dem Norddeutschen Rundfunk den Vorfall als erwartbar und forderte wirksamere Schutzmaßnahmen.

Besondere Brisanz erhält der Fall durch den neuen gesetzlichen Rahmen. Seit dem 17. März 2026 ist das KRITIS-Dachgesetz in Kraft, das die physische Resilienz kritischer Anlagen stärken soll. Der Drohnenfund am Flughafen Leipzig zeigt jedoch, dass bekannte Bedrohungen mit neuen gesetzlichen Vorgaben allein noch nicht beherrscht werden. Zwischen den Anforderungen an die Betreiber, den verfügbaren Schutzmaßnahmen und den tatsächlichen Möglichkeiten der Gefahrenabwehr bestehen weiterhin erhebliche Lücken.

Eine dieser Lücken betrifft ausgerechnet Drohnen. Eine konkrete Pflicht zu ihrer Detektion oder Abwehr enthält das KRITIS-Dachgesetz nicht, obwohl Fachleute dies bereits im Gesetzgebungsverfahren gefordert hatten. § 13 des Gesetzes regelt zwar die Resilienzpflichten kritischer Anlagen und die Erstellung verbindlicher Resilienzpläne, bleibt bei den konkreten Maßnahmen jedoch offen. Gefordert sind verhältnismäßige technische, sicherheitsbezogene und organisatorische Vorkehrungen auf Grundlage der jeweiligen Risikoanalyse. Damit liegt ein erheblicher Teil der Verantwortung bei den Unternehmen selbst: Sie müssen bekannte Gefahren bewerten und daraus angemessene Schutzmaßnahmen ableiten.

### Vom Gesetz zur Risikoanalyse

Das KRITIS-Dachgesetz verfolgt einen risikobasierten Ansatz. Betreiber kritischer Anlagen müssen die für ihre Anlagen relevanten Risiken analysieren und auf dieser Grundlage verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen treffen. Der mögliche Maßnahmenkatalog reicht dabei weit über klassischen Objektschutz hinaus. Genannt werden unter anderem Notfallvorsorge, physischer Schutz von Anlagen, Überwachung der Umgebung, Krisenmanagement, Alarmierungsverfahren und alternative Lieferketten. Neben der Prävention geht es um die Fähigkeit, die Folgen eines Vorfalls zu begrenzen und kritische Dienstleistungen nach einer Störung möglichst schnell wiederherzustellen. Wirtschaftsschutz umfasst deshalb den Schutz des Standorts ebenso wie die Vorbereitung auf mögliche Störungen. Wie schnell kann ein Unternehmen reagieren? Welche Prozesse müssen auch im Krisenfall weiterlaufen? Wie lässt sich der Betrieb nach einer Unterbrechung wieder aufnehmen?

Die Antworten auf diese Fragen gehören zunehmend zum Sicherheitskonzept eines Unternehmens bzw. Betriebs. Bei einem Flughafen wäre die Drohnendetektion beispielsweise nur ein Teil der Vorsorge. Ebenso relevant ist, welche Bereiche durch einen Vorfall beeinträchtigt werden könnten, wie der Betrieb bei einer Sperrung weitergeführt wird, welche Meldewege gelten und welche Sofortmaßnahmen vorhanden sind. Ähnliche Fragen stellen sich bei Sabotage, Stromausfällen oder anderen Störungen. Security


Management, Risikomanagement und Business Continuity Management greifen dabei ineinander. In vielen Unternehmen sind diese Aufgaben auf verschiedene Verantwortliche verteilt. Eine solche Arbeitsteilung funktioniert, wenn Risiken gemeinsam betrachtet werden und die Prozesse im Ereignisfall aufeinander abgestimmt sind.

Die praktische Umsetzung des KRITIS-Dachgesetzes befindet sich allerdings noch im Aufbau. Weitere Konkretisierungen, unter anderem zur Bestimmung kritischer Einrichtungen und zu methodischen Vorgaben für Risikoanalysen und Resilienzpläne, werden derzeit noch erarbeitet. Das Inkrafttreten des Gesetzes beantwortet daher noch längst nicht jede praktische Frage.

## NIS2 bringt die digitale Seite hinzu

Zusätzlich zum KRITIS-Dachgesetz hat NIS2 die Anforderungen an die Cybersicherheit erheblich ausgeweitet. Seit Dezember 2025 gilt das deutsche Umsetzungsgesetz, das deutlich mehr Unternehmen als die bisherige KRITIS-Regulierung erfasst. Besonders wichtige Einrichtungen müssen seitdem geeignete Maßnahmen zum Management ihrer Cybersicherheitsrisiken treffen und erhebliche Sicherheitsvorfälle melden.

NIS2 beziehungsweise das BSI-Gesetz und das KRITIS-Dachgesetz setzen an unterschiedlichen Stellen an. Während NIS2 vor allem die Sicherheit von Netz- und Informationssystemen regelt, richtet sich das KRITIS-Dachgesetz auf die physische Resilienz kritischer Anlagen. In der Praxis greifen beide Bereiche jedoch ineinander. Ein physischer Einbruch kann dem Zugriff auf IT-Systeme dienen, manipulierte digitale Berechtigungen können den Zutritt zu geschützten Bereichen ermöglichen. Auch ein Stromausfall betrifft häufig mehrere Ebenen gleichzeitig, von Produktionsanlagen über Server und Kommunikationssysteme bis hin zur elektronischen Sicherheitstechnik.

Für Unternehmen kommt es deshalb darauf an, diese Bereiche gemeinsam zu betrachten. Physische Sicherheit, Informationssicherheit, Risikomanagement und Business Continuity Management (BCM), also die Aufrechterhaltung kritischer Geschäftsprozesse bei Störungen, dürfen nicht nebeneinanderstehen. Sie müssen organisatorisch aufeinander abgestimmt werden. Große Konzerne können dafür meist auf spezialisierte Fachabteilungen zurückgreifen. Mittelständische Unternehmen müssen diese Anforderungen aber häufig mit deutlich geringeren personellen Ressourcen bewältigen.

## Mehr Verantwortung für die Geschäftsleitung

NIS2 und das KRITIS-Dachgesetz verankern die Verantwortung für Sicherheit ausdrücklich auf Leitungsebene. Geschäftsführungen müssen dafür sorgen, dass Risiken angemessen bewertet, erforderliche Maßnahmen beschlossen und deren Umsetzung kontrolliert werden. Technisches Detailwissen ist dafür nicht entscheidend, wohl aber die Fähigkeit, Sicherheitsfragen auf Managementebene zu verankern. Diese Verantwortung lässt sich nicht vollständig an Fachabteilungen oder externe Dienstleister übertragen. Dadurch gewinnen Sicherheitsinvestitionen auch regulatorisch und haftungsrechtlich an Gewicht. Unternehmen müssen nachvollziehbar darlegen können, auf welcher Grundlage sie Risiken bewertet und Schutzmaßnahmen ausgewählt haben. Versäumnisse können deshalb neben Betriebsunterbrechungen und Reputationsschäden auch rechtliche und finanzielle Folgen nach sich ziehen.

Wie weit Unternehmen bei der Vorsorge gehen müssen, hängt von den konkreten Risiken ihrer Anlagen ab. Das KRITIS-Dachgesetz schreibt deshalb keine maximalen Schutzmaßnahmen vor, sondern verlangt verhältnismäßige Lösungen. Wer eine bekannte Gefahr als weniger relevant einstuft oder auf eine bestimmte Schutzmaßnahme verzichtet, sollte diese Entscheidung fachlich begründen können. Die Dokumentation hält fest, wie Risiken bewertet und Schutzmaßnahmen ausgewählt wurden. Ob aber ein Sicherheitskonzept auch funktioniert, zeigt sich erst bei einem konkreten Vorfall, wenn Meldewege, Zuständigkeiten

und vorgesehene Maßnahmen tatsächlich greifen müssen.

### Beratungsbedarf wächst

Viele Unternehmen stehen aktuell vor der Herausforderung, aus den neuen gesetzlichen Vorgaben in konkrete Sicherheitsmaßnahmen umzusetzen, die auf sie zugeschnitten sind. Ein Energieversorger hat andere Risiken als ein Krankenhaus oder ein Logistikunternehmen und selbst innerhalb einer Branche unterscheiden sich oft technische Abhängigkeiten und betriebliche Abläufe. NIS2 und KRITIS-Dachgesetz geben dabei den Rahmen vor, die konkrete Ausgestaltung bleibt aber Aufgabe der Betreiber.

Damit wächst auch der Beratungsbedarf. Große Sicherheitsdienstleister unterstützen ihre Kunden bereits heute bei Risikoanalysen, Sicherheitskonzepten und der Krisenorganisation. Ihre Stärke liegt vor allem in der Kenntnis des Betriebsalltags: Sie wissen, wie ein Standort funktioniert, welche Meldewege tatsächlich genutzt werden und wo Abläufe im Ernstfall ins Stocken geraten können.

Diese Erfahrung wird nun auch für operative Sicherheitsdienste wichtiger. Wer Werk- oder Objektschutz übernimmt, muss wissen, welche Aufgaben bei einer Störung anfallen, wann Leitstelle oder Krisenstab eingeschaltet werden und welche Bereiche weiter gesichert werden müssen, wenn reguläre Systeme ausfallen. Sicherheitsdienstleister können so dazu beitragen, die Anforderungen aus NIS2 und KRITIS-Dachgesetz in praktikable Abläufe zu übertragen und bei Übungen oder im laufenden Betrieb zu prüfen, ob diese tatsächlich funktionieren.

# Analysen und Hilfestellungen zum Wirtschaftsschutz

**Von Rechtsanwalt Dr. Berthold Stoppelkamp**

**RA Dr. Berthold Stoppelkamp**
zuständiges Geschäftsführungsmitglied für den Fachausschuss Wirtschaftsschutz im BDSW

### BfV-Informationsblatt zum Schutz vor Ausspähung von Drohnen

Die Minimierung der Bedrohung durch Drohnen bleibt für die Wirtschaft eine Herausforderung und Daueraufgabe. Das Informationsblatt gibt Empfehlungen, wie Beschäftigte und Sicherheitsverantwortliche von Unternehmen eigenverantwortlich das eigene Schutzniveau erhöhen können.
**www.verfassungsschutz.de**

### UVB-Chatbot für Sicherheit und Resilienz

Im Rahmen der Unternehmerverbände Berlin-Brandenburg (UVB) – Wirtschaftsinitiative: Sicherheit und Resilienz ist der neue UVB-Chatbot online gegangen. Das KI-basierte Online-Tool unterstützt Unternehmen im Dialogformat mit wichtigen Informationen aus den Bereichen Energiesicherheit, Cybersecurity, Wirtschaftsschutz und Lieferkettenstabilität.
**www.uvb-online.de/uvb-chatbot-fuer-sicherheit-und-resilienz**

### PwC-Studie: Global Digital Trust Insights 2026

Zunehmende Unsicherheiten und der rasante technologische Wandel durch KI prägen auch das Umfeld der Cybersicherheit. 89 Prozent der befragten Unternehmen wurden in den letzten drei Jahren Opfer eines Datenzugriffs. Aufgrund des IT-Fachkräftemangels setzen mittlerweile 54 Prozent der Unternehmen KI-Tools in der Cybersicherheit ein.
**www.pwc.de/de/cyber-security/digital-trust-insights.html**

### Verfassungsschutzbericht 2025

Das extremistische Bedrohungspotenzial ist so groß wie noch nie und auf 58.700 Personen gestiegen. Nachrichtendienstliche Aktivitäten gegen Deutschland gingen schwerpunktmäßig von Russland, China und Iran aus. Politik, Militär, Wirtschaft und Wissenschaft sind dabei die Ausforschungs- und Manipulationsziele.
**www.verfassungsschutz.de**