Angriffe, die von oben kommen

Von Holger Köster

Holger Köster

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

Der Schutz Kritischer Infrastrukturen folgt seit Jahren klaren Prinzipien: Zutritt kontrollieren, Anlagen sichern, Prozesse überwachen. Viele dieser Maßnahmen sind erprobt und funktionieren zuverlässig – zumindest solange sich Bedrohungen innerhalb dieser bekannten Muster bewegen.

Doch das ist zunehmend nicht mehr der Fall. Kritische Infrastrukturen geraten heute aus unterschiedlichen Richtungen unter Druck. Neben Cyberangriffen und klassischen Sabotageakten rücken dabei vor allem Drohnen zunehmend in den Fokus. Sie ermöglichen Einblicke in sensible Bereiche, ohne physische Barrieren überwinden zu müssen. Gleichzeitig ist häufig unklar, wer sie steuert und mit welcher Absicht sie eingesetzt werden. Für die Verantwortlichen vor Ort entsteht daraus eine Situation, in der Vorfälle zwar erkannt, aber nicht immer eindeutig bewertet oder unmittelbar beantwortet werden können.

Hinzu kommen steigende regulatorische Anforderungen. Mit NIS2 und dem inzwischen verabschiedeten KRITIS-Dachgesetz werden Betreiber stärker in die Pflicht genommen, Risiken systematisch zu erfassen und Sicherheitsmaßnahmen nachvollziehbar zu organisieren.

Gerade im Umgang mit schwer einzuordnenden Vorfällen zeigt sich jedoch, wie anspruchsvoll diese Vorgaben in der Praxis sind. Denn klare Zuständigkeiten und definierte Prozesse treffen hier auf Lagen, die sich nicht immer eindeutig bewerten lassen. Damit rückt eine Frage stärker in den Mittelpunkt: Wie lassen sich Sicherheit und Reaktionsfähigkeit unter Bedingungen organisieren, in denen klassische Zuständigkeiten und Schutzmechanismen nicht mehr ausreichen?

Der folgende Beitrag greift diese Entwicklung auf und zeigt, welche konkreten Herausforderungen sich daraus für Betreiber kritischer Infrastrukturen ergeben und warum der Luftraum dabei eine wachsende Rolle spielt.

Ihr
Holger Köster

Bild: #642591136 / istockphoto.com

Drohnen über dem Werkstor

Warum sich Unternehmen kaum schützen können

Von Andreas Albrecht

Sie fliegen über Werften, Kraftwerke und Kliniken. Mal gezielt, mal scheinbar beiläufig und immer zahlreicher. Immer drängender stellt sich deshalb die Frage: Wer schützt eigentlich den Luftraum über Kritischer Infrastruktur?

Andreas Albrecht
Freier Fachredakteur und Journalist

In der Nacht zum 26. September 2025 wurden über Schleswig-Holstein mehrere Drohnen gesichtet, die über besonders sensible Einrichtungen flogen: über die U-Boot-Werft von Thyssen-Krupp Marine Systems, das Küstenkraftwerk, das Universitätsklinikum Kiel, die Raffinerie in Heide und auch über den Sitz der Landesregierung.

Die Sichtungen folgten auf ähnliche Vorfälle in Dänemark, wo kurz zuvor ebenfalls Drohnen über militärischen Anlagen und Kritischer Infrastruktur beobachtet worden waren. Auch deshalb leitete die Staatsanwaltschaft Flensburg Ermittlungen ein. Im Raum stand der Verdacht, der im Fachjargon „sicherheitsgefährdendes Abbilden" genannt wird – also gezielter staatlicher Spionage. Hätten sich die Hinweise bestätigt, könnten solche Aufnahmen dazu dienen, verwundbare Bereiche zu identifizieren: Munitionslager, kritische Anlagenstrukturen oder Bewegungsprofile von Personal. Doch eine eindeutige Antwort, wer für diese Drohnenflüge verantwortlich war und welchen Zweck sie verfolgten, steht bis heute aus.

Der Vorfall ist kein Einzelfall. In den vergangenen Monaten wurden immer wieder Drohnen über militärischen Anlagen, Industrieparks oder Energieinfrastrukturen gesichtet, häufig jedoch ohne eindeutige Zuordnung und selten mit konkreten Konsequenzen. Für die Verantwortlichen vor Ort stellen sich in solchen Situationen deshalb dringende Fragen: Wie können wir uns schützen? Wer ist zuständig? Und was darf im konkreten Fall überhaupt getan werden?

Zwischen Beobachtung und Handlungsgrenzen

Die Antworten auf diese Fragen fallen in der Praxis oft ernüchternd aus. In vielen Fällen bleibt es bei der Beobachtung und der Meldung an die zuständigen Stellen. Zwar gehen Sicherheitsbehörden regelmäßig davon aus, dass zumindest ein Teil der Drohnenflüge illegal ist. Gleichzeitig wird häufig betont, dass keine konkret gesteigerte Gefährdungslage vorliege. Diese Einschätzung mag im Einzelfall zutreffen, sie ändert jedoch nichts an der strukturellen Unsicherheit im Umgang mit solchen Vorfällen.

Denn selbst bei auffälligen Flugbewegungen lässt sich nur selten unmittelbar klären, ob es sich um Spionage, Vorbereitungshandlungen oder schlicht um die Neugier eines Hobbypiloten handelt. Auswertungen zeigen zwar, dass ein erheblicher Teil gemeldeter Drohnenflüge auf Privatpersonen zurückgeht, die ohne Genehmigung unterwegs sind. Doch es kann auch nicht ausgeschlossen werden, dass identische Flugmuster gezielt zur Informationsgewinnung genutzt werden.

Für Sicherheitsverantwortliche entsteht daraus eine schwierige Ausgangslage. Nicht jeder Vorfall ist sicherheitsrelevant, aber jeder muss zunächst ernst genommen werden. Die eigentliche Schwierigkeit zeigt sich jedoch erst nach der Sichtung: Selbst wenn eine Drohne erkannt wird, bleibt oft unklar, wer zuständig ist und welche Maßnahmen überhaupt erlaubt sind.

Der Luftraum als offene Flanke

Die Vorfälle machen deutlich, dass klassische Schutzkonzepte an Grenzen stoßen, sobald Beobachtung oder Störung aus der Luft erfolgt. Zäune, Zugangskontrollen oder Perimeterschutzsysteme sind auf Bedrohungen am Boden ausgelegt. Drohnen umgehen diese Barrieren mühelos. Sie ermöglichen Einblicke in Bereiche, die bislang als geschützt galten, und können Bewegungen, technische Strukturen und Abläufe erfassen.

Vor diesem Hintergrund wurden die Vorfälle in Schleswig-Holstein früh als Teil hybrider Bedrohungsszenarien eingeordnet. Neben möglicher Aufklärung geht es dabei auch um das Testen von Reaktionsfähigkeit und das bewusste Ausnutzen struktureller Schwächen.

Dabei zeigt sich ein bemerkenswerter Widerspruch: Die technische Erkennung funktioniert


Bild: # 2214636470 / istockphoto.com

zunehmend besser. Polizei, Betreiber und Sicherheitsdienste registrieren ungewöhnliche Flugbewegungen und können sie dokumentieren. Die eigentliche Schwäche liegt inzwischen weniger im Erkennen als vielmehr im Reagieren.

Koordination ohne Wirkung?

Mit dem Gemeinsamen Drohnenabwehrzentrum in Berlin hat der Bund Ende 2025 versucht, an dieser Stelle anzusetzen. Ziel war es, Informationen zu bündeln, Lagebilder schneller zu erstellen und die Zusammenarbeit zwischen den Behörden zu verbessern.

Tatsächlich hat sich die Koordination seitdem verbessert. Sichtungen werden systematischer erfasst, Entwicklungen lassen sich besser nachvollziehen. An der eigentlichen Problemlage ändert das jedoch wenig. Denn das Drohnenzentrum selbst greift nicht ein, die operative Verantwortung bleibt bei den Behörden vor Ort.

Das führt zu einem zentralen Widerspruch: Die Lage wird besser erkannt, aber nicht schneller oder konsequenter bewältigt. Die bekannten Fälle der vergangenen Monate verdeutlichen das. Mehrfach wurden Drohnen über längere Zeiträume hinweg beobachtet, etwa im Januar 2026 über dem Nord-Ostsee-Kanal oder auf militärischen Übungsplätzen. In diesen Situationen lagen ausreichend Informationen vor, um den Vorfall zu bewerten. Dennoch blieb eine wirksame Reaktion aus.

Wenn Zuständigkeiten zum Problem werden

Ein wesentlicher Grund dafür liegt in den fragmentierten Zuständigkeiten, die auf verschiedene Behörden verteilt sind und je nach Einsatzort wechseln können. Ein Beispiel macht das deutlich: Wird eine Drohne außerhalb eines Flughafengeländes gesichtet, ist zunächst die Landespolizei zuständig. Fliegt sie auf das Gelände, geht die Verantwortung auf die Bundespolizei über. Verlässt sie den Bereich wieder, wechselt die Zuständigkeit erneut. Und fliegt die Drohne über eine militärische Anlage, ist weder Bundes- noch Landespolizei verantwortlich, sondern die Bundeswehr.

Das heißt, dass eine Drohne unter Umständen innerhalb weniger Sekunden mehrere Zuständigkeitsbereiche durchqueren kann. In der Praxis bedeutet das: Während eine Drohne beobachtet wird, muss zunächst geklärt werden, wer überhaupt eingreifen darf. Doch bis diese Klärung erfolgt ist, hat sich die Lage häufig bereits verändert. Die Drohne ist weitergeflogen oder verschwunden.

Der IT-Sicherheitsexperte Manuel Atug, Sprecher der Arbeitsgemeinschaft KRITIS, die sich seit Jahren mit dem Schutz Kritischer Infrastrukturen beschäftigt, hat diese Struktur treffend als „Wimmelbild der Verantwortungsdiffusion“ beschrieben. Gemeint ist ein System, in dem Zuständigkeiten formal geregelt sind, im konkreten Fall jedoch nicht schnell genug greifen und völlig unpraktikabel sind.

Technik, die nicht genutzt werden darf

Hinzu kommt ein weiteres Spannungsfeld, nämlich die Diskrepanz zwischen technischen Möglichkeiten und rechtlichem Rahmen. Die Detektion von Drohnen ist heute technisch an sich gut lösbar. Sensorik, Radar und optische Systeme ermöglichen eine frühzeitige Erkennung und Verfolgung. Problematisch ist aber die Frage, wie darauf reagiert werden darf.

Viele wirksame Gegenmaßnahmen sind rechtlich stark eingeschränkt. Funkstörsysteme, mit denen Drohnen kontrolliert oder zur Landung gezwungen werden könnten,

unterliegen in Deutschland strengen rechtlichen Beschränkungen und sind für Unternehmen in der Praxis nicht einsetzbar und auch ein Abschuss ist nur unter extremen Voraussetzungen zulässig und mit erheblichen Risiken verbunden.

Neue Anforderungen, neue Rollenverteilung?

Für Betreiber Kritischer Infrastrukturen ergibt sich daraus eine schwer kalkulierbare Lage. Risiken sind sichtbar, lassen sich aber nicht in jedem Fall unmittelbar kontrollieren. Ein vollständiger Schutz vor Drohnen ist unter diesen Bedingungen kaum realistisch. Entscheidend ist daher weniger die vollständige Verhinderung, sondern der professionelle Umgang mit solchen Vorfällen. Unternehmen müssen in der Lage sein, Drohnensichtungen einzuordnen, schnell zu reagieren und betriebliche Abläufe auch unter Störung aufrechtzuerhalten.

Dafür müssten der Luftraum Teil der Risikoanalyse werden und organisatorische Fragen noch deutlicher an Gewicht gewinnen: Wer meldet einen Vorfall? Wer bewertet ihn? Wer entscheidet über das weitere Vorgehen? Und wie greifen diese Prozesse im Ernstfall ineinander?

Doch viele, vor allem mittelständische Betreiber, können diese Aufgaben nicht allein bewältigen, weder personell noch organisatorisch. Die private Sicherheitswirtschaft könnte hier Unterstützung bieten. Sie ist in vielen Fällen die erste Instanz vor Ort, kennt die individuellen betrieblichen Abläufe ihrer Kunden und könnte technische Systeme, organisatorische Prozesse und operative Maßnahmen zusammenführen.

Denn gerade im Umgang mit Drohnen zeigt sich, dass Sicherheit nicht mehr allein durch einzelne Maßnahmen gewährleistet werden kann. Gefragt sind integrierte Konzepte, die Erkennung, Bewertung und Reaktion miteinander verbinden.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

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

BBK-Broschüre: Vorsorgen für Krisen und Katastrophen

Extreme Wetterereignisse nehmen zu. Durch Cyberattacken, Desinformation oder Sabotage finden Angriffe auf Infrastrukturen, Meinungsbildung und Zusammenhalt statt. Selbst ein Krieg scheint nicht mehr so ausgeschlossen zu sein wie noch vor einigen Jahren. Diese Broschüre unterstützt, wie man Extremsituationen möglichst sicher meistert.
www.bbk.bund.de

BfV-Sicherheitshinweis für die Wirtschaft 1/2026: Energiesektor im Visier

Der Sicherheitshinweis des BfV ordnet die aktuelle Gefährdungslage für den deutschen Energiesektor durch Spionage, Sabotage und gewaltbereiten Extremismus ein und gibt praxisnahe Empfehlungen, mit denen Personal- und (IT-)Sicherheitsverantwortliche sowie Beschäftigte eigenverantwortlich das eigene Schutzniveau erhöhen können.
www.verfassungsschutz.de

Cybersicherheitsmonitor 2026

Künstliche Intelligenz (KI) ist im digitalen Alltag omnipräsent. Das nutzen Cyberkriminelle für Onlinebetrug. Der Cybersicherheitsmonitor 2026 des BSI und des Programms Polizeiliche Kriminalprävention des Bundes und der Länder zeigt, wie hoch das Risiko ist, Opfer digitaler Betrugsmaschen zu werden.
www.bsi.bund.de

DIN SPEC 14027 Corporate Security Grundschutz

Das Dokument schließt die bisherige Lücke eines Standards für die physische Sicherheit von Unternehmen, Konzernen und anderen Organisationen. Das Dokument bietet umfangreiche Anforderungskataloge zu verschiedenen Bereichen wie beispielsweise Reisesicherheit, Continuity Management, Standortsicherheit und zum Know-how-Schutz.
www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2026/03/din-spec-corporate-security.html