Zwischen Bedrohung und Schutz: Wirtschaft im Fokus

Von Holger Köster

Holger Köster

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

Ein Unternehmen entwickelt Hochtechnologie – und wird ausspioniert. Eine Drohne kreist über einem Umspannwerk – und niemand fühlt sich zuständig. Ein Produktionsnetz wird gehackt – und eine ganze Lieferkette bricht zusammen. Was wie Einzelfälle klingt, ist leider längst Teil einer systematischen Bedrohungslage.

Spionage und Sabotage haben sich in den letzten Jahren rasant professionalisiert. Sie zielen nicht mehr nur auf Staatsgeheimnisse, sondern auf wirtschaftliche Schlüsselressourcen, auf technologische Vorsprünge oder auf Kritische Infrastrukturen. Und sie treffen uns dort, wo wir am verletzlichsten sind: im Vertrauen auf funktionierende Abläufe, gesicherte Informationen, geschützte Räume.

Der Staat hat mit Gesetzen wie NIS2 und dem KRITIS-Dachgesetz reagiert, Sicherheitsbehörden wie das Bundesamt für Verfassungsschutz (BfV) oder das Bundesministerium für Wirtschaft und Energie (BMWK) bieten der Wirtschaft Unterstützung an. Doch oft fehlt es noch an Umsetzungskraft und Klarheit. So wird der Schutz der Wirtschaft zu einem Kraftakt, der ohne verlässliche Partner nicht zu stemmen ist.

Private Sicherheitsdienstleister können solche Partner sein. Sie kennen die Abläufe vor Ort, verstehen die Risiken aus dem operativen Alltag und können zwischen Anspruch und Wirklichkeit vermitteln. Aber sie brauchen Spielräume, klare Regeln und das Vertrauen, dass ihre Rolle mehr ist als Objektschutz.

Wie diese Rolle aussehen kann und wie der Schutz der Wirtschaft heute neu gedacht werden könnte, zeigt der Beitrag auf den folgenden Seiten.

Ihr
Holger Köster

Bild: # 1979406539 / istockphoto.com

Schwachstellen im System

Warum der Schutz vor Spionage und Sabotage oft Stückwerk bleibt

Von Andreas Albrecht

Die Bedrohung durch Spionage, Sabotage und gezielte Einflussnahmen ist real und sie betrifft längst nicht mehr nur Behörden oder Ministerien. Sicherheitsbehörden berichten seit 2025 von einer massiven Zunahme hybrider Angriffe, die sich längst auch gegen private Unternehmen richten, vom kleinen Mittelständler über Betreiber Kritischer Infrastrukturen bis hin zu börsennotierten Konzernen.

Andreas Albrecht
Freier Fachredakteur
und Journalist

Handelt es sich bei den Angriffen nicht um Erpressungsversuche (Ransomware), bleiben die Interessen der oft unbekannten Angreifer meist im Dunkeln. Geht es um geistiges Eigentum? Um Marktkenntnisse? Um Zugang zu Produktionsanlagen? Oder doch um gezielte Destabilisierung kritischer Infrastruktur durch Staaten, die es nicht gut mit Deutschland meinen? Gerade weil die Motive oft unklar sind, wird ein umfassenderes Schutzkonzept immer dringlicher, das staatliche Prävention, unternehmerische Eigenverantwortung und die Rolle der privaten Sicherheitswirtschaft effektiv miteinander verzahnt.

Staatliche Initiativen: viel Angebot, wenig Struktur

Immerhin: Politik und Sicherheitsbehörden haben das Thema Wirtschaftsschutz mittlerweile deutlich stärker auf der Agenda als noch vor wenigen Jahren. Das Bundesamt für Verfassungsschutz (BfV) etwa widmet der Wirtschaftsspionage ein eigenes Kapitel im jährlichen Verfassungsschutzbericht. Dort werden regelmäßig konkrete Fallbeispiele dokumentiert, etwa Spionageversuche im Hochtechnologiebereich oder strategisch motivierte Aktivitäten ausländischer Nachrichtendienste im Umfeld von KI, Halbleitertechnik oder Energieversorgung. Im Bundesministerium für Wirtschaft und Energie (BMWK) wurde das Referat Wirtschaftsschutz etabliert. Mit der Initiative WISIND („Wirtschaftsschutz-Initiative Deutschland“) stellt das Ministerium Handlungsempfehlungen, Leitfäden und Ansprechpartner vor allem für kleine und mittlere Unternehmen bereit. Und auch das BfV bietet Workshops, Schulungen und Checklisten für Unternehmen an, die sich gegen Ausspähung und Sabotage wappnen wollen.

Doch aus Sicht vieler Unternehmen fehlt es bei den gut gemeinten Angeboten an Struktur und Zugänglichkeit. Wer sich informieren will, steht häufig vor einem Dschungel an PDF-Dokumenten von Anträgen und redundanten Angeboten. Zudem klaffen Anspruch und Wirklichkeit oft auseinander. Die viel zitierte „vertrauensvolle Zusammenarbeit von Staat und Wirtschaft“ bleibt häufig ein Lippenbekenntnis und in der Praxis Stückwerk. Die zahlreichen Maßnahmen und Unterstützungsangebote sind oft schlecht oder überhaupt nicht koordiniert und Unternehmen klagen über unklare Zuständigkeiten, hohe bürokratische Hürden und mehrere verschiedene Ansprechpartner. Gerade für mittelständische Betriebe mit begrenzten personellen Ressourcen stellt dies eine große Herausforderung dar.

Fallbeispiel Drohnenabwehrzentrum Berlin: Anspruch und Realität

Ein Beispiel für die Diskrepanz zwischen politischem Anspruch und operativer Umsetzung ist das neue Drohnenabwehrzentrum in Berlin. Ende 2025 als zentrale Koordinationsstelle angekündigt, sollte es der zunehmenden Bedrohung durch unbemannte Flugobjekte Rechnung tra-

Bild: # 690772190 / istockphoto.com

gen. Die Realität sieht bislang jedoch ernüchternd aus, zumindest aus Sicht vieler Sicherheitsverantwortlicher in der Wirtschaft.

Kritik entzündet sich vor allem an zwei Punkten: Erstens ist das Zentrum aus Sicht vieler Praktiker kaum mehr als eine symbolpolitische Maßnahme ohne echte Wirkung. Zweitens bleiben zentrale Fragen der Zuständigkeit ungeklärt: Wer ist bei einem konkreten Drohnenvorfall verantwortlich? Was darf ein Sicherheitsdienstleister, was eine Landes- oder Bundespolizei? Und welche technischen Mittel stehen überhaupt zur Verfügung?

Bild: # 1915205991 / istockphoto.com

Ein konkretes Beispiel, das die Komplexität der Problematik verdeutlicht, gibt ein Vertreter eines großen deutschen Sicherheitsunternehmens, das so geht: Fliegt eine Drohne in Richtung eines Zuges, liegt die Zuständigkeit bei der Bundespolizei, da Gleisanlagen unter deren Hoheit fallen. Eine Landespolizei dürfe hier gar nicht eingreifen – selbst dann nicht, wenn sie direkt vor Ort wäre. Gleichzeitig sei es derzeit rechtlich nicht verboten, mit einer Drohne über Privatbesitz oder das Gelände Kritischer Infrastrukturen zu fliegen.

Aus Sicht des Experten müsste die Politik hier dringend nachsteuern, insbesondere durch eine Ausweitung des sogenannten Hausrechts für Betreiber Kritischer Infrastrukturen. Nur wenn Unternehmen selbst rechtssicher handeln dürfen, etwa durch den Einsatz technischer Gegenmaßnahmen oder notfalls durch die Abwehr feindlicher Drohnen, könne effektiver Schutz gewährleistet werden.

Sabotage, Lieferketten, unklare Schnittstellen: neue Angriffsflächen

Während Spionage gezielt auf Know-how und Daten zielt, richtet sich Sabotage oft gegen die Funktionsfähigkeit von Produktions- oder Versorgungssystemen. Hier geraten zunehmend auch indirekte Angriffspunkte in den Blick: Subunternehmer, Dienstleister, schlecht gesicherte digitale Schnittstellen oder veraltete Maschinenparks mit ungepatchten Softwaresystemen.

Die Komplexität moderner Lieferketten und das hohe Maß an digitaler Vernetzung eröffnen Angreifern zahlreiche Möglichkeiten, mit vergleichsweise geringem Aufwand großen Schaden anzurichten. NIS2 und andere regulatorische Vorgaben wie das jüngst beschlossene KRITIS-Dachgesetz zielen daher verstärkt auf die gesamte Wertschöpfungskette, inklusive der Berücksichtigung der physischen Sicherheit.

Social Engineering: Wenn der Mensch das Einfallstor ist

Eine weitere, oft unterschätzte Bedrohung geht vom sogenannten Social Engineering aus: Angreifer versuchen hier, über menschliche Schwächen Zugang zu Informationen oder Systemen zu erlangen, sei es über gefälschte E-Mails, manipulierte Anrufe oder physische Einschleusung in Unternehmen, indem sich die Täter als interne IT-Abteilungen, externe Dienstleister oder sogar Behörden ausgeben.

Abhilfe schaffen hier nur konsequente Awareness-Schulungen, ein klar geregeltes Rechtemanagement und eine Sicherheitskultur, die auf Wachsamkeit und klare Zuständigkeiten setzt. Auch hier ist die Unterstützung durch externe Fachleute sinnvoll, etwa in Form von Workshops, Testszenarien oder individuell zugeschnittenen Präventionskonzepten.

Private Sicherheitswirtschaft: Brücke zwischen Staat und Wirtschaft

Eine wichtige Rolle beim Schutz vor Spionage und Sabotage spielt die private Sicherheitswirtschaft. Ihre Aufgabe ist es zunehmend nicht nur, zu schützen, sondern auch zu beraten, zu koordinieren und technische wie organisatorische Maßnahmen umzusetzen. Diese Rolle wird vor allem im Umfeld Kritischer Infrastrukturen an Bedeutung gewinnen.

Viele große Sicherheitsdienstleister übernehmen heute bereits diese Verantwortung, beraten zu moderner Sicherheitstechnik, Schnittstellenabsicherung oder Notfallmanagement. Die Herausforderung liegt darin, diese Kompetenzen auch in der Fläche verfügbar zu machen, insbesondere für mittelständische Unternehmen oder Betreiber kleinerer KRITIS-relevanter Einrichtungen.

Neben dem klassischen Objektschutz gehören heute auch technische Sicherheitslösungen, IT-nahe Dienstleistungen, Risikoanalysen und die Unterstützung bei der Umsetzung regulatorischer Anforderungen zum Leistungsportfolio einiger Sicherheitsfirmen. Voraussetzung dafür ist neben technischer Expertise vor allem ein tiefes Verständnis für rechtliche Rahmenbedingungen und operative Abläufe im Kundenumfeld.

Zwischen Anspruch und Wirklichkeit: Der Handlungsdruck wächst

Der Schutz der deutschen Wirtschaft vor Spionage und Sabotage ist eine gesamtgesellschaftliche Aufgabe. Staatliche Initiativen wie das BfV, das BMWK mit WISIND oder das neue Drohnenabwehrzentrum setzen wichtige Impulse – bleiben aber oft hinter den operativen Erwartungen zurück. Der Gesetzgeber muss dringend für mehr Klarheit bei Zuständigkeiten und Eingriffsrechten sorgen.

Gleichzeitig liegt es an den Unternehmen selbst, ihre Widerstandsfähigkeit zu erhöhen. Die neue gesetzliche Lage (NIS2, KRITIS-Dachgesetz) bietet hierfür einen klaren Handlungsrahmen. Wer sich nicht nur auf gesetzliche Mindeststandards verlässt, sondern frühzeitig in Beratung, Technik und Schulung investiert, gewinnt nicht nur Sicherheit, sondern auch Resilienz.

Die private Sicherheitswirtschaft kann dabei zum entscheidenden Bindeglied werden: zwischen politischen Vorgaben und betrieblicher Praxis, zwischen Prävention und Reaktion, zwischen technischer Umsetzung und strategischer Beratung. Es ist an der Zeit, diese Rolle weiter zu stärken, zum Schutz der deutschen Wirtschaft in einer zunehmend komplexen und vor allem gefährdeten Welt.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

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

BBK: Vorsorge- und Hilfestellungen bei Stromausfall

Wie der lang anhaltende großflächige Stromausfall zu Beginn des Jahres in Berlin gezeigt hat, kommt das gesamte private und geschäftliche Leben zum Erliegen. Es kommt kein Wasser. Internet, Bargeldautomaten und Mobilfunk sind gestört. Das BBK gibt Tipps und Informationen zur Vorsorge und Krisenbewältigung.
www.bbk.bund.de

BfV: Hintergrundinformationen zu Angriffen von Linksextremisten auf Kritische Infrastrukturen (KRITIS) und Wirtschaftsunternehmen

Bestimmte Wirtschaftsbereiche stehen besonders im Fokus von Linksextremisten, da sie als tragende Säulen des „ausbeuterischen" und „repressiven kapitalistischen Systems" betrachtet werden. Bei Angriffen auf KRITIS ist zu berücksichtigen, dass Unternehmen vielfach Aufgaben im Rahmen der Grundversorgung übernehmen.
www.verfassungsschutz.de

VORSORGEPLAN für Krisen, Katastrophen, Konflikte

Der neu von der Handelskammer Hamburg gemeinsam mit dem BBK entwickelte Krisenvorsorgeplan hilft Unternehmen aller Größenklassen dabei, Risiken im Unternehmen systematisch zu identifizieren, kritische Abläufe abzusichern, Verantwortlichkeiten klar zu regeln, Notfallkommunikation vorzubereiten und Störungen schneller zu überstehen.
www.handelskammer-hamburg.de/international-aussenwirtschaft/vorsorgeplan-6812560

Whitepaper: Corporate Resilience

Der Think Tank „Corporate Resilience" der Technischen Hochschule Ingolstadt hat ein Whitepaper zu den wirtschaftlichen Folgen hybrider Bedrohungen für Unternehmen und ihre Wertschöpfungsketten erstellt. Dieses enthält branchenspezifische Handlungsempfehlungen, um in volatilen Sicherheitslagen wettbewerbsfähig zu bleiben.
www.vsw-bundesverband.de/downloads/studien-umfragen/