Foto: KI generiert

Vier KRITIS-Sektoren – ein Schutzauftrag: Energie, Gesundheit, Logistik und Verteidigung können nur mit einem ganzheitlichen Ansatz abgesichert werden.

# Vier Sektoren, ein Schutzauftrag

## Energie, Healthcare, Logistik und Defence stehen unter Druck. Das KRITIS-Dachgesetz legt Standards fest, doch echte Resilienz gelingt nur ganzheitlich.

Wir leben in einer neuen Sicherheitsrealität. Sabotageakte und Cyberangriffe verdeutlichen, dass Resilienz kein reines Expertenthema mehr ist, sondern zur gemeinsamen Verpflichtung von Staat und Wirtschaft wird. Mit dem KRITIS-Dachgesetz schreibt die Bundesregierung ab 2026 erstmals bundesweite Mindeststandards für physische Sicherheit und Krisenvorsorge vor.

Resilienz entsteht im Zusammenspiel aller Akteure.

Genau hier setzt die SDM GROUP aus München an.

„Resilienz bedeutet für uns mehr als der Schutz vor einzelnen Risiken", betont Jens-Peter Neumann, CEO der SDM GROUP. „Unser Anspruch ist es, Systeme so zu planen, zu testen und zu betreiben, dass sie auch unter extremen Belastungen funktionieren – nicht nur auf dem Papier, sondern im realen Einsatz." Der Claim „Wir schützen

Deutschland“ steht dabei für einen ganzheitlichen Ansatz, der Betreiber, Behörden und Sicherheitsdienstleister gleichermaßen in die Pflicht nimmt.

## Neue Dimension der Bedrohung

Betreiber Kritischer Infrastrukturen spüren aktuell, dass das Bedrohungsspektrum keinen Halt vor Zuständigkeitsgrenzen macht. Staatlich gesteuerte hybride Bedrohungen reichen von Cyberangriffen über Sabotage bis hin zu Desinformation. „Die Bedrohungslage in Deutschland hat eine neue Dimension erreicht“, warnt Generalleutnant a.D. Andreas Hoppe, ehemaliger Stellvertreter des Generalinspekteur der Bundeswehr und externer Senior Advisor der SDM GROUP. Feindliche Dienste und Extremisten nähmen gezielt Schwachstellen ins Visier – ob Verkehrsknoten, Stromtrassen oder Kommunikationsnetze. Die Verwundbarkeit vernetzter Systeme steigt, Resilienz wird zum Prüfstein für Staat, Wirtschaft und Gesellschaft.

## Vier Säulen für den KRITIS-Schutz

Neumann fordert deshalb ein Umdenken: „Hybride Angriffe betreffen IT, industrielle Steuerung, physische Anlagen und Informationsflüsse zugleich.“ Die Antwort liege in integrierten Sicherheitskonzepten, in denen Sensorik, Prozesse und Einsatzkräfte ein gemeinsames Lagebild erzeugen und schnell reagieren können. Resilienz entsteht damit im Zusammenspiel aller Akteure – vom Betreiber über Behörden bis zum spezialisierten Sicherheitsdienstleister als strategischem Partner.

SDM positioniert sich entsprechend als „Resilienz-Partner“ für Betreiber Kritischer Infrastrukturen und bündelt ihre Leistungen in vier strategischen Säulen: Defence, Logistics, Energy und Healthcare. Ziel ist es, die Funktionsfähigkeit zentraler Versorgungs- und Sicherheitssektoren auch unter Krisendruck aufrechtzuerhalten. Parallel betreut das Unternehmen weiterhin seine langjährigen Kunden in privaten und öffentlichen Bereichen.

## Sektor Verteidigung: Schutz für Bundeswehr und Rüstungsindustrie

Bundeswehr und Defence-Industrie sind längst ins Visier ausländischer Akteure gerückt. Ein Vorfall sorgte 2024 für Schlagzeilen: US-Geheimdienste deckten einen geplanten russischen Anschlag auf Rheinmetall-CEO Armin Papperger auf und vereitelten ihn gemeinsam mit deutschen Stellen. „Zur klassischen kritischen Infrastruktur muss auch die Defence-Industrie gezählt werden“, betont Generalleutnant a.D. Hoppe.

„Resilienz bedeutet für uns mehr als der Schutz vor einzelnen Risiken.“

**Jens-Peter Neumann,** CEO der SDM GROUP

Foto: privat

Neben Spionage und Sabotage rückt vor allem die Gefahr durch Drohnen in den Fokus, die immer öfter über Kasernen oder Übungsplätzen gesichtet werden. Die Antwort darauf sind Drohnenabwehr-Systeme in Hand ziviler Sicherheitskräfte. Der Qualitätsanspruch ist klar: Der Schutz militärischer Liegenschaften und Rüstungsbetriebe erfordert heute eine enge Verzahnung von technischer Integration, hochprofessionellem Objektschutz und einer 24/7 Überwachung auf höchstem Niveau. Konkret bedeutet das: bewaffnete Wachmannschaften, deren Ausbildungsstand dem von Soldaten entspricht, modernste Sensorik und effektive Drohnenabwehr. SDM setzt hierbei auf Personal mit Bundeswehr-Hintergrund und Übungen unter Realbedingungen.

Auch im Objektschutz vollzieht sich ein Wandel von bloßer Präsenz hin zu proaktiver Gefahrenabwehr. Dazu gehört die Kontrolle aller Umfeldfaktoren – vom Zugangsschutz über Backgroundchecks des Personals bis zur digitalen Überwachung kritischer Anlagen. Der Schutz kritischer militärischer Akteure ist Teil der nationalen Resilienz.

## Sektor Healthcare: Verwundbarkeit der Kliniken

Krankenhäuser galten lange als unantastbare Zufluchtsorte. Doch in Zeiten hyb- ▶

Foto: SDM GROUP

Blick in einen Krankenhausflur bei Nacht: Krankenhäuser gelten nicht länger als sichere „Schonräume“ – sie müssen auf Krisenfälle vorbereitet werden.

Foto: SDM GROUP

Strom und Energie als Lebensader moderner Gesellschaften: Das Energiesystem ist ein bevorzugtes Ziel für Sabotage – ein Ausfall hätte weitreichende Folgen für Bevölkerung und Wirtschaft.

Foto: SDM GROUP

Ein Rüstungsbetrieb ohne Absicherung: Moderne Drohnenabwehr und ständige Wachsamkeit werden für Produktionsstandorte der Defence-Industrie essenziell.

rider Konflikte ist das Gesundheitswesen verwundbarer als gedacht. Eine aktuelle Analyse im Auftrag der Deutschen Krankenhausgesellschaft kommt zu einem alarmierenden Befund: Im Krisen- oder Kriegsfall wären deutsche Krankenhäuser aufgrund von Personalengpässen und Mängeln in der physischen Sicherheit nur bedingt einsatzfähig. Viele Häuser verfügen weder über ausreichende Zugangskontrollen noch über belastbare Notfallpläne für Sabotage- oder Terrorlagen.

„Krankenhäuser dürfen nicht länger als ungefährdete zivile Zonen gelten – das wäre ein gefährlicher Irrglaube", warnt Neumann, der selbst lange Jahre CFO der Rhön-Klinikum Gruppe war. „Wenn die zivile Versorgung zum Ziel wird, brauchen wir robuste Schutzkonzepte, die weit über Brandschutztüren hinausgehen." Erfahrungen aus der Pandemie und dem Ukraine-Krieg zeigen, dass Kliniken Teil der nationalen Sicherheitsvorsorge sind. Dennoch weisen Umfragen auf Defizite hin: ungetestete Notstromaggregate, fehlende Evakuierungspläne und leicht zu überlistende Zutrittssysteme. Hinzu kommen Hackerangriffe, wie der Ransomware-Vorfall an einer Uniklinik 2020 zeigte.

Die SDM GROUP plädiert für einen Paradigmenwechsel. Gemeinsam mit der Versicherungswirtschaft entwickelt das Unternehmen ganzheitliche Sicherheitsaudits. „Resilienz im Krankenhaus heißt, auch im Ausnahmezustand funktionsfähig zu bleiben", erklärt Neumann. Das umfasst Notfallkommunikation ohne öffentliche Netze, geschützte Vorräte (Medikamente und Diesel) sowie trainierte Krisenstäbe. Erste Erfolge gibt es bereits: Ein Uniklinikum in NRW rüstet – beraten von SDM-Experten – Pforten mit Personenschleusen nach. Die Botschaft ist klar: Gesundheitseinrichtungen sind Kritische Infrastruktur – ihr Schutz ist Teil der inneren Sicherheit.

„Lager, Depots und Transporte sichern wir bislang oft nur physisch, aber nicht strukturell."

**Andreas Schindler,**
CSO der SDM GROUP

Foto: SDM GROUP

## Sektor Logistik: Sicherheit für Lager und Lieferketten

Ohne funktionierende Logistik steht das Land still. Die Verteilung von Militärgütern, Medikamenten oder Lebensmitteln gleicht einem verwundbaren Nervensystem. Wie gravierend Sicherheitslücken sein können, zeigte ein Fall im sächsischen Burg: Unbekannte entwendeten aus einem unbewacht abgestellten LKW rund 20.000 Schuss Bundeswehr-Munition.

„Lager, Depots und Transporte sichern wir bislang oft nur physisch, aber nicht strukturell", kritisiert Andreas Schindler, CSO der SDM GROUP. „Es stehen Zäune und Kameratürme, doch es fehlt ein durchgängiges Sicherheitskonzept von der Halle bis zur Haustür." In vielen Logistikzentren mangelt

es an lückenlosen Zugangskontrollen oder Sicherheitsüberprüfungen von Fahrern und Subunternehmern. Auch die Routenplanung erfolgt selten unter Sicherheitsaspekten. Gleichzeitig lassen sich Lieferketten gezielt stören – etwa durch Angriffe auf Verkehrsinfrastruktur oder durch eingeschleuste Insider.

SDM setzt deshalb auf ganzheitliche Supply-Chain-Sicherheit. Gemeinsam mit Unternehmen werden Risikoanalysen für jedes Glied der Kette erarbeitet. Zentrale Knotenpunkte – Häfen, Frachtzentren, Distributionslager – können so priorisiert gesichert werden. Videoüberwachung mit KI-gestützter Auswertung soll auffällige Bewegungsmuster automatisiert melden. Zusätzlich gewinnt Insiderprävention an Bedeutung: Mitarbeitende in sicherheitskritischen Bereichen werden gezielt sensibilisiert, um etwa Social-Engineering-Angriffe früh zu erkennen.

Schindler betont zudem den Faktor Redundanz: „Resilienz heißt auch, Alternativen zu haben." Wenn ein Lager sabotiert oder ein Transportweg blockiert ist, braucht es Ausweichoptionen – etwa zweite Standorte, Notfall-Lieferverträge oder abgesicherte Routen. SDM berät Logistiker bei der Konzeption solcher Fallback-Strukturen. Der Aufwand ist erheblich, der Nutzen jedoch sektorübergreifend: Logistiksicherheit wirkt als Multiplikator, weil nahezu alle KRITIS-Bereiche auf stabile Lieferketten angewiesen sind.

## Sektor Energie: Verwundbare Lebensadern sichern

Die Energieversorgung ist hochgradig komplex und anfällig. Ein Blackout hätte dramatische Folgen: Verkehr, Kommunikation und Wasserversorgung kämen zum Erliegen. Dass dies keine Theorie ist, zeigte jüngst ein Stromausfall in Berlin-Steglitz, bei dem 45.000 Haushalte und Krankenhäuser im Dunkeln saßen.

„Die Angriffspunkte sind vielfältig: Abgelegene Umspannwerke und kilometerlange Überlandleitungen lassen sich oft schon mit einfachen Mitteln sabotieren", erklärt CSO Schindler. Auch Gaspipelines und Windparks sind potenzielle Ziele. Er warnt: „Da Karten kritischer Knotenpunkte teils öffentlich verfügbar sind und Notfallpläne fehlen, reicht oft wenig Know-how für dramatische Effekte."

SDM begegnet diesen Risiken mit integrierten Schutzlösungen für Energieanlagen.

„Zur klassischen kritischen Infrastruktur muss auch die Defense-Industrie gezählt werden."

**Andreas Hoppe,** ehemaliger Stellvertreter des Generalinspekteurs der Bundeswehr und externer Senior Advisor der SDM GROUP

Foto: privat

Im Sektor Energy unterstützt das Unternehmen unter anderem Netz- und Kraftwerksbetreiber sowie Leitstellen dabei, Infrastrukturen robuster aufzustellen – etwa durch Sensorsysteme, die Annäherungen detektieren (Bewegungssensorik, Wärmebildkameras, Drohnendetektion) und definierte Interventionsketten auslösen. Ergänzend berät SDM beim Aufbau von Notfallkapazitäten und bei der Verzahnung von Technik, Personal und Prozessen.

## Die SDM GROUP als Systempartner für nationale Resilienz

Das KRITIS-Dachgesetz ist ein Meilenstein, kann aber nur der Anfang sein. Es braucht einen Kulturwandel: Weg vom Silo-Denken, hin zur echten Zusammenarbeit zwischen Betreibern, Staat und Sicherheitsdienstleistern. Dafür sind Investitionen in Technik, Ausbildung und gemeinsame Lagezentren nötig. Diese zahlen sich aus, wenn dadurch auch nur ein einziger großer Blackout oder Anschlag verhindert wird.

Die Leitfrage lautet nicht mehr „Wer schützt was?", sondern „Wie schützen wir gemeinsam unser Land?". Im Schulterschluss aller Beteiligten liegt der Schlüssel – oder, um es mit dem Anspruch von SDM zu sagen: Wir schützen Deutschland. Gemeinsam, strategisch und mit Weitblick. ■

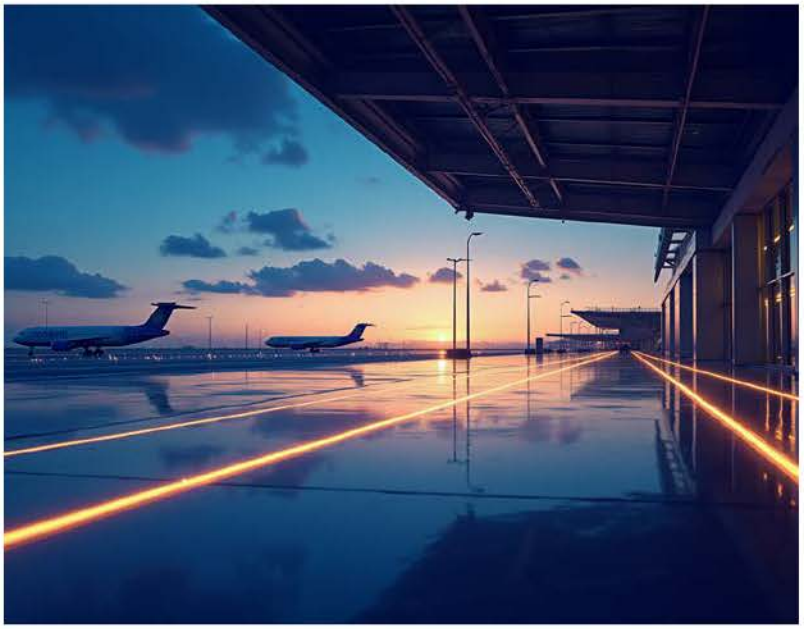

Foto: SDM GROUP

Nächtlicher Blick auf einen Airport-Logistik-Hub: Transportflugzeuge stehen bereit – doch wie gut sind Perimeter und Transporte vor Diebstahl oder Sabotage geschützt?