



Kritische Infrastruktur und Industrie

Sicher und resilient in Krisenzeiten

In Zeiten hybrider Angriffe ist erhöhte Wachsamkeit gefragt. Bei kritischer Infrastruktur und in der Industrie steigen die Anforderungen an robuste technische Sicherheitskonzepte. Unabhängige Prüfungen werden zum systemrelevanten Faktor.

Bedrohliche Drohnenüberflüge, gezielte Sabotageakte: Die geopolitische Zuspitzung hat Deutschland erreicht – und Angreifer nehmen verstärkt die Infrastruktur ins Visier. Experten sprechen von einer aus dem Ausland gesteuerten „hybriden Kriegsführung“: Physische und digitale Attacken stellen die Wehrhaftigkeit des Landes auf die Probe. Cyberangriffe legen Betriebe und Lieferketten lahm. Insbesondere kritische Infrastruktur (KRITIS) wie Energieversorgungsanlagen, Kliniken, Rechenzentren und Pipelines

werden zu potenziellen Zielen. Wie folgenschwer ein Sabotageakt sein kann, wurde im Januar in Berlin klar. Unbekannte hatten eine Kabelbrücke am Teltowkanal in Brand gesetzt. Die Schwachstelle im System war präzise gewählt: In 45.000 Haushalten und 2.000 Betrieben fielen über Tage Strom und Heizung aus. Krankenhäuser mussten evakuiert werden. Insgesamt registrierte das Bundeskriminalamt nach Medienberichten im Jahr 2025 in Deutschland insgesamt 321 Sabotageverdachtsfälle. Einbrü-

che in Umspannwerke oder Windenergieanlagen und gefährliche Eingriffe in den Zugverkehr werden registriert. 1.289 verdächtige Drohnenüberflüge wurden aktenkundig.

15%

der Industriebetriebe haben einen Werkschutz installiert.

IW-Umfrage 2025

Es gilt, sich zu wappnen: Umfassende Schutzkonzepte und belastbare Sicherheitsprüfungen werden insbesondere für Betreiber von KRITIS-Anlagen permanent nachgeschärft. Das Bundesinnenministerium installiert im

Bundesamt für Verfassungsschutz ein neues Abwehrzentrum gegen hybride Bedrohungen.

Die staatlichen Stellen sind alarmiert. Doch nicht überall in Wirtschaft und Gesellschaft sei das Ausmaß der Bedrohung vollständig erkannt, warnt Hubertus Bardt, Geschäftsführer des Instituts der deutschen Wirtschaft

(IW). „Es muss für alle deutlicher werden, dass es sich hier

nicht um abstrakte theoretische Szenarien handelt. Es geht um Risiken, die eine gewisse Eintrittswahrscheinlichkeit haben.“ Auch die Privatwirtschaft müsse mehr Resilienz zeigen – und für den Ernstfall gewappnet sein. „Die

Wirtschaft muss laufen – nicht nur vor einem militärischen Konflikt, sondern auch während einer konkreten Krise.“

Eine Umfrage des IW aus dem Spätherbst 2025 belegt eine Schiefelage der Abwehrstrategien: Während immerhin 86 Prozent der Industriebetriebe nach eigener Auskunft Schutzmaßnahmen gegen Cybergefahren ergreifen, wappnen sich nur 54 Prozent gegen Sabotage, 52 Prozent gegen Spionage und nur knapp 15 Prozent haben einen Werkschutz installiert. Befragt wurden mehr als 1.000 Geschäftsführer. Unternehmen müssten über Cybersicherheit hinausdenken, fordert Bardt: „Bei Drohnenüberflügen wissen die Betriebe im Einzelnen nicht, ob es sich um Spionage handelt oder nur um das Spielzeug des Jungen von nebenan. Trotzdem müssen sie darauf reagieren.“ Denn klar ist auch:



Moderne Gesellschaften sind in hohem Maße von stabiler Technik abhängig. Und Resilienz entsteht durch robuste technische Anlagen, die dauerhaft gesichert und gewartet und regelmäßig unabhängig geprüft werden. „Unabhängige Prüfungen sind das entscheidende Bindeglied zwischen einem sicheren Betrieb und einer übergreifenden Lagebeurteilung“, sagt Guido Kehmer, Geschäftsfeldmanager Aufzüge und Fördertechnik bei TÜV Rheinland.

Unabhängige Prüfer sind in ganz Deutschland für die Begutachtung Tausender Energieanlagen, Pipelines, Speicher explosiver hochentzündlicher Stoffe und Industrieanlagen verantwortlich. Kehmer plädiert für Konzepte, die über das Klein-Klein hinausgehen: „In den letzten Jahren haben wir die Tendenz festgestellt, dass Anlagenbetreiber zwar einzelne Komponenten prüfen lassen, aber mitunter Gefahr laufen, das Gesamtbild zu übersehen.“ Unabhängige

Prüfer könnten genau die nötigen Verknüpfungen herstellen. „Wir sehen die Robustheit einer Anlage nicht nur unter dem Aspekt der Ausfall- und Verwendungssicherheit, sondern nehmen auch die Angreifbarkeit von außen in den Blick.“

Dabei rücken heute auch Dinge in den Fokus, die vor einigen Jahren noch keine Beachtung fanden. So erklärt es Ralf Schmitt, Leiter des Kompetenzzentrums Elektro- und Gebäudetechn-



nik beim TÜV Rheinland: „Wie zugänglich ist eigentlich eine Anlage? Wie leicht gelangt man an eine Steuerung, um eine Manipulation durchzuführen?“ Solche Fragen zählten traditionell nicht zum klassischen Prüfauftrag der zugelassenen Überwachungsstellen, sondern sie liegen in der Betreiberverantwortung. Dennoch würden sie immer stärker nachgefragt. Auch

bar, denn bisher konnte dort bestenfalls ein Vogel landen. Wenn nun aber eine Drohne angefliegen kommen kann, muss man neu beurteilen.“ Das Umdenken habe begonnen – unter Einbeziehung unabhängiger Prüfer als Kontrollinstanz und Partner. Mit wachsender technischer Komplexität und zunehmender Vernetzung von Anlagen häufen sich die Risiken.

Betreiber technische mit organisatorischen Maßnahmen. „Bei den Audits wird regelmäßig überprüft, ob die Maßnahmen zueinander passen und ineinandergreifen. So bekommt man die Komplexität in den Griff“, sagt Kehmer.

Auch die Zuverlässigkeit des Personals ist in Sachen Gefahrenabwehr immer wichtiger: Wer hat zu sicherheitsrelevanten Bereichen Zugang? Wer darf an Steuerungen, Prozessleitsystemen und Netzwerkkomponenten hantieren? Wie genau werden Dienstleister aus Wartungs- und Instandhaltungsfirmen auf ihre Zuverlässigkeit abgeklopft? Manches liegt hier noch im Graubereich: „Der klassische Arbeitsschutz geht zunächst nicht von einem Innentäter aus“, erklärt Schmitt. Somit muss der Betreiber laut technischen Regeln selber bewerten, ob er einen möglichen Innentäter in der Gefährdungsbeurteilung berücksichtigt oder nicht.

„Unabhängige Prüfungen sind das entscheidende Bindeglied zwischen einem sicheren Betrieb und einer übergreifenden Lagebeurteilung.“

Guido Kehmer
Geschäftsfeldmanager Aufzüge und Fördertechnik
TÜV Rheinland

Penetrationstests mit freundlich gesinnten Hackern werden von TÜV-Spezialeinheiten im Kundenauftrag durchgeführt, um Schwachstellen zu identifizieren.

Schmitt erkennt einen Wandel im Prüfalltag, der der veränderten Weltlage Rechnung trägt. „Natürlich steht bei uns noch immer das technische Versagen im Vordergrund – also beurteilen wir Faktoren wie Alterung, Verschleiß, Ausfallwahrscheinlichkeit.“ Doch mit den hybriden Bedrohungen entstünden zusätzliche Gefahren, sei es durch kriminelle Handlungen oder staatlich organisierte Drohszenarien. Die zugespitzte Weltlage zwingt zum Umdenken. Schmitt nennt das Beispiel eines großen Tanklagers einer Chemieanlage: „Wenn sich oben auf dem Tanklager ein explosionsgefährdeter Bereich befindet, war das beherrscht-

Gleichzeitig wird aber der Ruf nach Bürokratieabbau in der Wirtschaft lauter. „Die Politik möchte Betreiber auch größerer Anlagen gerne entlasten und gewährt mehr Freiheiten“, sagt Kehmer. Er betrachtet den Trend, sich mit eigenverantwortlichen Wartungen zu begnügen, mit Skepsis. „Die Kompetenz einer unabhängigen Prüfgesellschaft ist es, über den Tellerrand hinauszublicken.“ Unabhängige Prüfungen seien die zentrale Voraussetzung für die Anlagensicherheit. Schmitt betont die Bedeutung einer ganzheitlichen Sicht. „Die Summe von vielen Einzelmaßnahmen ergibt noch keine sichere Anlage.“ Um auf dem Feld der Cybersicherheit diesem Ziel näher zu kommen, bieten sich bei hochkomplexen Anlagen spezielle Audits an. Mit sogenannten Managementsystemen zur Informationssicherheit (ISMS) kombiniert ein