(Foto: Krass99 - Stock.Adobe.com)

16.03.2026

# Resilienz und Wirtschaftsschutz – Warum Unternehmen jetzt krisenfest werden müssen

Deutschlands kritische Infrastruktur ist erschreckend verwundbar – und das nutzen Angreifer aus, wie die jüngsten Anschläge auf die Stromversorgung in Berlin gezeigt haben: Im Herbst 2025 fiel der Strom in einem Berliner Technologiepark aus, Anfang 2026 mussten rund 45.000 Haushalte und 2.200 Betriebe teils tagelang ohne Strom und Heizung auskommen. Sogar Abschnitte des Mobilfunknetzes fielen aus. Solche Ereignisse können die gesamte Wirtschaft einer Region im Handumdrehen lahmlegen – und das sind leider keine Einzelfälle: Vermehrt seit 2022 kommt es europaweit immer wieder zu Sabotageakten auf Energie- oder Datenkabel, es gibt Drohnensichtungen über kritischen oder militärischen Anlagen und Cyberangriffe auf Unternehmen. Der andauernde Krieg in der Ukraine, der Konflikt im Nahen Osten und erhebliche geopolitische Spannungen weltweit wirken sich spürbar auf die Wirtschaft aus.Für deutsche Unternehmen bedeutet das: Ihre Krisenpläne müssen auf den Prüfstand – und ihre Geschäftsmodelle widerstandsfähiger werden. (Link: https://www.dihk.de/resource/blob/153592/25f8df1924640992aef44807851f1e3d/wirtschaftspolitik-dihk-position-verteidigung-2025-data.pdf)

**Mehr Sicherheit kostet – und lohnt sich am Ende dann doch**
Betriebswirtschaftlich betrachtet führt Resilienz zunächst zu höheren Kosten und Ineffizienzen, beispielsweise wegen des Aufbaus eines größeren Lieferantennetzwerks oder des Einkaufs von Sicherheitstechnik beziehungsweise Notstromaggregaten. Auch die Einstellung von (IT-)Sicherheitsexperten oder die Einrichtung von Meldewegen und Krisenplänen bedeutet anfangs Mehraufwand. In einem Ernst- oder Katastrophenfall entscheidet aber ein etabliertes Krisenmanagement darüber, ob Produktion und Logistik weiterlaufen können – oder ob ein Betrieb sogar völlig zum Stillstand kommt.

Für Unternehmen, die über belastbare Krisenstrukturen verfügen, ist Resilienz vor allem eines: ein Wettbewerbsvorteil. Wer gegen Attacken und Störungen gerüstet ist, bleibt wirtschaftlich handlungsfähig. Derart gewappnete Unternehmen sind attraktive Kooperationspartner. Das gilt insbesondere für Betriebe, die Partner der Sicherheits- und Verteidigungsindustrie sind oder es werden wollen. Denn gerade in dieser Branche zählt absolute Zuverlässigkeit. Auftraggeber erwarten stabile Lieferketten, den Schutz sensibler Daten und eine Produktion, die auch unter Druck und erst recht im Krisenfall funktioniert.

Eines ist dabei wichtig zu verstehen: Es geht nicht darum, auf jede Eventualität vorbereitet zu sein. Es kommt vielmehr darauf an, die betriebseigenen Schwachstellen zu kennen, identifizierte Risiken zu minimieren und im Ernstfall schnell reagieren zu können.

**KRITIS: Neue Mindeststandards für kritische Infrastrukturen**

Mit dem sogenannten KRITIS-Dachgesetz, das Bundestag und Bundesrat gerade beschlossen haben, soll der Schutz „kritischer Infrastruktur“ gestärkt werden. Dazu zählen etwa Energieversorger, Lebensmittelhersteller und Transportunternehmen. Das Gesetz legt Mindestanforderungen für Betreiber kritischer Anlagen fest. Sie müssen zum Beispiel Notfallteams bilden, Objektschutz garantieren und Maßnahmen zur Ausfallsicherheit ergreifen. Darüber hinaus werden sie verpflichtet, Sicherheitsvorfälle beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu melden. Aus diesen Meldungen erstellt das BBK „anlassbezogene Lagebilder“ zur aktuellen Gefährdungslage und stellt diese den zuständigen Behörden und Anlagenbetreibern, etwa Energieversorgern, zur Verfügung. Aus Sicht der DIHK sollte geprüft werden, ob das BBK solche Lagebilder nicht allen Unternehmen zugänglich machen kann. Denn für viele Betriebe können solche konkreten Lagebilder ein wirkungsvoller Anreiz, mehr in die eigene Resilienz zu investieren: Sie könnten so Bedrohungen leichter identifizieren und ihr Krisenmanagement entsprechend anpassen.

Im KRITIS-Dachgesetz beträgt der Schwellenwert für kritische Anlagen grundsätzlich „500.000 von einer Anlage zu versorgende Einwohner“. Im parlamentarischen Gesetzgebungsverfahren hat der Bundestag nun festgelegt, dass die Bundesländer über diesen Richtwert hinaus weitere Anlagen als „kritisch“ einstufen können.

Ergänzt wurde zudem, dass die KRITIS-Resilienzstrategie den Betreibern kritischer Infrastruktur bislang auferlegte Transparenzpflichten hinterfragen soll. Gerade im sicherheitsrelevanten Bereich und kritischen Anlagen kann zu viel Transparenz nämlich neue Risiken schaffen. Öffentlich einsehbare Informationen einzelner Transparenzpflichten lassen sich, ähnlich einem Mosaik, sogar zu einem Gesamtbild zusammenfügen, das Angriffsflächen für Cyberattacken, Sabotage oder Spionage bietet. Die Wirtschaft kann zahlreiche Hinweise einbringen, welche Regelungen angepasst werden sollten – zum Beispiel im Energie- beziehungsweise Baurecht oder bei Informationsgesetzen.

**Wirtschaftsschutz als neuer Fokus in der Wirtschaftspolitik**

Die Bundesregierung setzt mit ihrer „Nationalen Wirtschaftsschutzstrategie“ und der darin angekündigten Kooperation mit den Unternehmen ein wichtiges Signal. Sie betont die Verantwortung der Wirtschaft für die Entwicklung resilienter Geschäftsmodelle. Entscheidend ist dabei, dass die Bundesregierung einem Ansatz folgt, der insgesamt die wirtschaftspolitischen Rahmenbedingungen für die hiesigen Betriebe im Blick hat. Denn nur bei entsprechenden unternehmerischen Freiheiten werden Unternehmen in eine stärkere Resilienz investieren können. Deshalb sollte vor allem auf weitere Regulierung und Mindeststandards verzichtet und auf das Eigeninteresse der Wirtschaft gesetzt werden.

Auch die IHK-Organisation geht hier voran: Die DIHK ist aktives Mitglied der „Initiative Wirtschaftsschutz“ des Bundesministeriums des Innern. In Kooperation mit den Behörden und den Verbänden der Initiative entwickelt die DIHK Informationsmaterialien für Unternehmen und organisiert Veranstaltungen zur sicherheitspolitischen Lage. Und sie setzt sich für klare Regeln ein, die den Betrieben eine belastbare Personalplanung ermöglichen – denn auch das gehört zur Vorsorge. So sollte es den Unternehmen möglich sein, in ihrer Belegschaft zu fragen, wer sich als Reservist beziehungsweise Reservistin oder bei zivilen Hilfsorganisationen engagiert. Bislang wissen das nur sehr wenige Unternehmen – auch, weil ein entsprechender Rechtsrahmen fehlt. Doch nur mit solchen Informationen lassen sich krisenbedingte personelle Ausfälle realistisch einschätzen.

## Resilienz und Wirtschaftsschutz – Warum Unternehmen jetzt krisenfest werden müssen

Deutschlands kritische Infrastruktur ist erschreckend verwundbar – und das nutzen Angreifer aus, wie die jüngsten Anschläge auf die Stromversorgung in Berlin gezeigt haben: Im Herbst 2025 fiel der Strom in einem Berliner Technologiepark aus, Anfang 2026 mussten rund 45.000 Haushalte und 2.200 Betriebe teils tagelang ohne Strom und Heizung auskommen. Sogar Abschnitte des Mobilfunknetzes fielen aus. Solche Ereignisse können die gesamte Wirtschaft einer Region im Handumdrehen lahmlegen – und das sind leider keine Einzelfälle: Vermehrt seit 2022 kommt es europaweit immer wieder zu Sabotageakten auf Energie- oder Datenkabel, es gibt Drohnensichtungen über kritischen oder militärischen Anlagen und Cyberangriffe auf Unternehmen. Der andauernde Krieg in der Ukraine, der Konflikt im Nahen Osten und erhebliche geopolitische Spannungen weltweit wirken sich spürbar auf die Wirtschaft aus. Für deutsche Unternehmen bedeutet das: Ihre Krisenpläne müssen auf den Prüfstand – und ihre Geschäftsmodelle widerstandsfähiger werden.

### Mehr Sicherheit kostet – und lohnt sich am Ende dann doch

Betriebswirtschaftlich betrachtet führt Resilienz zunächst zu höheren Kosten und Ineffizienzen, beispielsweise wegen des Aufbaus eines größeren Lieferantennetzwerks oder des Einkaufs von Sicherheitstechnik beziehungsweise Notstromaggregaten. Auch die Einstellung von (IT-)Sicherheitsexperten oder die Einrichtung von Meldewegen und Krisenplänen bedeutet anfangs Mehraufwand. In einem Ernst- oder Katastrophenfall entscheidet aber ein etabliertes Krisenmanagement

darüber, ob Produktion und Logistik weiterlaufen können – oder ob ein Betrieb sogar völlig zum Stillstand kommt.

Für Unternehmen, die über belastbare Krisenstrukturen verfügen, ist Resilienz vor allem eines: ein Wettbewerbsvorteil. Wer gegen Attacken und Störungen gerüstet ist, bleibt wirtschaftlich handlungsfähig. Derart gewappnete Unternehmen sind attraktive Kooperationspartner. Das gilt insbesondere für Betriebe, die Partner der Sicherheits- und Verteidigungsindustrie sind oder es werden wollen. Denn gerade in dieser Branche zählt absolute Zuverlässigkeit. Auftraggeber erwarten stabile Lieferketten, den Schutz sensibler Daten und eine Produktion, die auch unter Druck und erst recht im Krisenfall funktioniert.

Eines ist dabei wichtig zu verstehen: Es geht nicht darum, auf jede Eventualität vorbereitet zu sein. Es kommt vielmehr darauf an, die betriebseigenen Schwachstellen zu kennen, identifizierte Risiken zu minimieren und im Ernstfall schnell reagieren zu können.

KRITIS: Neue Mindeststandards für kritische Infrastrukturen

Mit dem sogenannten KRITIS-Dachgesetz, das Bundestag und Bundesrat gerade beschlossen haben, soll der Schutz „kritischer Infrastruktur“ gestärkt werden. Dazu zählen etwa Energieversorger, Lebensmittelhersteller und Transportunternehmen. Das Gesetz legt Mindestanforderungen für Betreiber kritischer Anlagen fest. Sie müssen zum Beispiel Notfallteams bilden, Objektschutz garantieren und Maßnahmen zur Ausfallsicherheit ergreifen. Darüber hinaus werden sie verpflichtet, Sicherheitsvorfälle beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu melden. Aus diesen Meldungen erstellt das BBK „anlassbezogene Lagebilder“ zur aktuellen Gefährdungslage und stellt diese den zuständigen Behörden und Anlagenbetreibern, etwa Energieversorgern, zur Verfügung. Aus Sicht der DIHK sollte geprüft werden, ob das BBK solche Lagebilder nicht allen Unternehmen zugänglich machen kann. Denn für viele Betriebe können solche konkreten Lagebilder ein wirkungsvoller Anreiz, mehr in die eigene Resilienz zu investieren: Sie könnten so Bedrohungen leichter identifizieren und ihr Krisenmanagement entsprechend anpassen.

Im KRITIS-Dachgesetz beträgt der Schwellenwert für kritische Anlagen grundsätzlich „500.000 von einer Anlage zu versorgende Einwohner“. Im parlamentarischen Gesetzgebungsverfahren hat der Bundestag nun festgelegt, dass die Bundesländer über diesen Richtwert hinaus weitere Anlagen als „kritisch“ einstufen können.

Ergänzt wurde zudem, dass die KRITIS-Resilienzstrategie den Betreibern kritischer Infrastruktur bislang auferlegte Transparenzpflichten hinterfragen soll. Gerade im sicherheitsrelevanten Bereich und kritischen Anlagen kann zu viel Transparenz nämlich neue Risiken schaffen. Öffentlich einsehbare Informationen einzelner Transparenzpflichten lassen sich, ähnlich einem Mosaik, sogar zu einem Gesamtbild zusammenfügen, das Angriffsflächen für Cyberattacken, Sabotage oder Spionage bietet. Die Wirtschaft kann zahlreiche Hinweise einbringen, welche Regelungen angepasst werden sollten – zum Beispiel im Energie- beziehungsweise Baurecht oder bei Informationsgesetzen.

Wirtschaftsschutz als neuer Fokus in der Wirtschaftspolitik

Die Bundesregierung setzt mit ihrer „Nationalen Wirtschaftsschutzstrategie“ und der darin angekündigten Kooperation mit den Unternehmen ein wichtiges Signal. Sie betont die Verantwortung der Wirtschaft für die Entwicklung resilienter Geschäftsmodelle. Entscheidend ist dabei, dass die Bundesregierung einem Ansatz folgt, der insgesamt die wirtschaftspolitischen Rahmenbedingungen für die hiesigen Betriebe im Blick hat.

Denn nur bei entsprechenden unternehmerischen Freiheiten werden Unternehmen in eine stärkere Resilienz investieren können. Deshalb sollte vor allem auf weitere Regulierung und Mindeststandards verzichtet und auf das Eigeninteresse der Wirtschaft gesetzt werden.

Auch die IHK-Organisation geht hier voran: Die DIHK ist aktives Mitglied der „Initiative Wirtschaftsschutz“ des Bundesministeriums des Innern. In Kooperation mit den Behörden und den Verbänden der Initiative entwickelt die DIHK Informationsmaterialien für Unternehmen und organisiert Veranstaltungen zur sicherheitspolitischen Lage. Und sie setzt sich für klare Regeln ein, die den Betrieben eine belastbare Personalplanung ermöglichen – denn auch das gehört zur Vorsorge. So sollte es den Unternehmen möglich sein, in ihrer Belegschaft zu fragen, wer sich als Reservist beziehungsweise Reservistin oder bei zivilen Hilfsorganisationen engagiert. Bislang wissen das nur sehr wenige Unternehmen – auch, weil ein entsprechender Rechtsrahmen fehlt. Doch nur mit solchen Informationen lassen sich krisenbedingte personelle Ausfälle realistisch einschätzen.

## ANSPRECHPARTNER

Innovation, Umwelt, Energie

CHRISTIAN KIEN

Tel.: 0651 9777-540
kien@trier.ihk.de