Öffentlicher Sektor - Zukunft gestalten Blog
By PwC Deutschland | 09. Juli 2026

# Unternehmen müssen Resilienz in ihrer Strategie verankern

**Eine neue Studie von Strategy& und der BAKS beschreibt, wie Privatunternehmen zu mehr Resilienz beitragen können.**

Cyberangriffe auf Behörden und Unternehmen, Sabotage an Unterseekabeln in der Ostsee, orchestrierte Desinformationskampagnen: Deutschlands Bedrohungslage hat sich in den vergangenen Jahren grundlegend verändert. Hybride Angriffe treffen den Staat, die Wirtschaft und die Zivilgesellschaft gleichzeitig.[AD1.1] Die aktuelle Studie „Business into breach“ von Strategy& und der Bundesakademie für Sicherheitspolitik (BAKS) analysiert, welche Rolle die Privatwirtschaft bei der zivilen Verteidigung spielen kann – und sollte. Der Hintergrund: Unternehmen betreiben kritische Infrastruktur, von Energienetzen über Rechenzentren bis hin zur Transportlogistik. Sie stellen Cybersicherheitslösungen bereit und beschäftigen Reservist:innen und Ehrenamtliche. Dennoch sind sie bisher nicht ausreichend in die nationale Sicherheitsarchitektur eingebunden. Die Studie identifiziert acht zentrale Herausforderungen für die Privatwirtschaft, den öffentlichen Sektor und die Zivilgesellschaft. Im privaten Sektor wiegt eine besonders schwer: Viele Vorstände behandeln Krisenfestigkeit lediglich als Compliance-Aufgabe, integrieren sie aber nicht in Investitionsentscheidungen und die Unternehmensstrategie. Wie existenzbedrohend diese Lücke werden kann, zeigt der Cyberangriff auf den Automobilhersteller Jaguar Land Rover Ende August 2025. Geschätzter Schaden: 2,1 Milliarden Euro.

Dabei rechnet sich Krisenfestigkeit auch finanziell: 87 Prozent aller deutschen Unternehmen waren dem Digitalverband Bitkom zufolge im Jahr 2025 Ziel von Cyberattacken. Allein IT-Ausfälle kosten europäische Firmen jährlich rund vier Milliarden Euro. Diese Kosten senkt, wer in Resilienz investiert. Und: Unternehmen, die Verfügbarkeitsgarantien oder Sicherheitszertifizierungen vorweisen können, erschließen neue Märkte und differenzieren sich effektiv von Wettbewerbern. Nicht zuletzt ist Krisenfestigkeit bei vielen öffentlichen Auftraggebern ein Vergabekriterium – etwa bei Vorhalteverträgen der Bundeswehr mit der Deutschen Bahn.

**Koordinationslücken schließen**

Hinzu kommt, dass es zwischen Unternehmen kaum systematischen Austausch über Bedrohungen und Schutzmaßnahmen gibt. Organisatorische Silos – von der IT über die Produktion bis hin zum Sicherheitsbereich – verhindern häufig eine durchgängige Strategie. Dies betrifft kleine und mittlere Unternehmen (KMUs) besonders; sie verfügen selten über professionelle Business-Continuity-Strukturen und führen das Thema „nebenbei“ im Qualitätsmanagement oder in der IT-Abteilung mit. Lückenhaft ist auch die Koordination zwischen Staat und Wirtschaft. Zwar existieren Plattformen wie die Allianz für Cybersicherheit des Bundesamts für Sicherheit in der Informationstechnik und das Nationale Cyber-Abwehrzentrum. Doch der Austausch ist häufig technisch, auf einzelne Branchen begrenzt und erreicht den Mittelstand kaum.

**Vorbild aus Großbritannien**

Abhilfe schaffen können Entscheider:innen mit zwölf Maßnahmen – fünf von ihnen adressieren die Privatwirtschaft. An erster Stelle steht, Resilienz in den CEO-Agenden zu verankern, um Krisenfestigkeit in Strategie, Governance und operative Prozesse einzubetten. Ebenso müssen Unternehmen innovative Technologien wie KI-gestützte Risikoerkennung und moderne Verschlüsselung einsetzen – nicht nur aufgrund gesetzlicher Vorgaben, sondern als Schutzmaßnahme und strategischer Wettbewerbsvorteil.

Ein weiterer Hebel ist ehrenamtliches Engagement der Mitarbeiter:innen: Unternehmen sollten Mitarbeiter:innen, die sich bei der Feuerwehr, dem Technischen Hilfswerk und Rettungsdiensten engagieren, gezielt fördern und ihre Kompetenzen nutzen, um die betriebliche Krisenfähigkeit zu stärken. Zugleich sollten sie Reservist:innen organisatorisch einbinden – mit festen Ansprechpartner:innen in den Personalabteilungen und Vertretungsregelungen für den Fall einer Einberufung.

Als Vorbild kann der britische „Defence Employer Recognition Scheme“ dienen: Dieser zeichnet Arbeitgeber aus, die Reservist:innen unterstützen. Rund 5.000 britische Unternehmen haben diese Auszeichnung seit 2015 bereits erhalten. Deutschlands „Partner der Reserve“-Programm erreicht nur einen Bruchteil davon. Für den öffentlichen Sektor sollte der Nationale Sicherheitsrat seine koordinierende Funktion stärker ausüben. Der Rat sollte insbesondere die fragmentierte Regulierungslandschaft – NIS-2, DORA, BSI-Grundschutz, KRITIS-Dachgesetz – in einheitliche Leitlinien überführen. Außerdem braucht Deutschland ein standardisiertes System für Echtzeit- Lagebilder auch mit Daten aus dem privaten Sektor; bislang fehlt die Transparenz über die Gesamtlage. Das geplante Nationale Lagezentrum könnte Abhilfe schaffen – vorausgesetzt, die automatisierte Datenanbindung und klare Governance-Regeln sind sichergestellt.

Das dritte Handlungsfeld ist die Zivilgesellschaft, bei der insbesondere Vereine, Verbände und Gewerkschaften als Multiplikatoren wirken sollten. Aktive Ehrenamtliche könnten als „Resilienz-Botschafter:innen“ in Schulen und Betrieben auftreten. Zudem muss die Medienkompetenz systematisch gestärkt werden – in Finnland beispielsweise ist sie in den Lehrplänen eine von sieben Kernkompetenzen – von der Grundschule bis zur Erwachsenenbildung.

Sehr sinnvoll sind darüber hinaus sektorübergreifende Krisenübungen. Bislang finden Übungen mit Beteiligung des privaten Sektors zu sporadisch statt. Komplexe Szenarien, die Cyberangriffe, physische Störungen und Desinformation gleichzeitig simulieren, fehlten fast vollständig. Klare Anreize könnten Unternehmen zur Teilnahme bewegen – ein „Resilienz-Partner“-Siegel etwa könnte bei öffentlichen Ausschreibungen als Qualifikation dienen. Auch die Kooperation zwischen Wirtschaft und Sicherheitsbehörden müsse enger werden. Für KMUs könnte ein „Security Liaison Officer“ als feste:r Ansprechpartner:in fungieren.

**Wirkungsvolle Sofortmaßnahmen**

Folgende Sofortmaßnahmen könnten Resilienz rasch stärker bei Unternehmen verankern: Sie sollten klare Zuständigkeiten schaffen – etwa eine:n Krisenansprechpartner:in, der oder die direkt an den Vorstand berichtet. Sie sollten zudem einen Resilienz-Schnellcheck durchführen: keine umfassende Analyse, sondern eine realistische Bewertung der wichtigsten Verwundbarkeiten bei Prozessen, Lieferketten, IT-Systemen und Üersonalabhängigkeiten. Zudem sollten sie regionale Austauschformate zwischen Unternehmen, Kommunen und Rettungsdiensten etablieren. Und die Bevölkerung sollte Kenntnisse zu Desinformation und Selbstvorsorge erwerben.

Die Finanzierung kann dabei auf bestehenden Instrumenten aufbauen: kommunale Mittel für

Gefahrenvorsorge, Förderprogramme für Cybersicherheit und europäische Fonds. Dies auch im Hinblick auf die NATO-Verpflichtung, bis 2035 die Verteidigungsausgaben – inklusive Mitteln für Zivil- und Infrastrukturverteidigung – auf fünf Prozent des BIP zu steigern.

Lesen sie mehr in der **Studie**.

**Ansprechpartner:**
**Prof. Dr. Rainer Bernnat**

**Zu weiteren PwC Blogs**

**Schlagwörter**

Artificial Intelligence (AI), Compliance, Digitalisierung, IT-Sicherheit, IT-Systeme, Small and Medium Enterprises (SME)

**Kontakt**

**Prof. Dr. Rainer Bernnat**
Frankfurt am Main
rainer.bernnat@pwc.com