THINKTANK
CORPORATE RESILIENCE
EXECUTIVE SUMMARY CSO

Wirtschaftliche Folgen hybrider Bedrohungen für Unternehmen und ihre Wertschöpfungsketten – Wie muss sich die Wirtschaft jetzt vorbereiten?

VSW
Bundesverband

LEAD.SECURE.SHAPE RESILIENCE
THI
MBA STRATEGY, GLOBAL RISK AND SECURITY MANAGEMENT

Dezember 2025

Executive Summary Chief Security Officers

Hybride Kriegsführung: Strategische Neuausrichtung der Unternehmenssicherheit

Deutschland befindet sich in einer Phase militärisch-hybrider Intensivierung. Corporate Security wird damit vom Schutzdienstleister zum strategischen Enabler der Unternehmensresilienz und zur operativen Schnittstelle zwischen Wirtschaft, Staat und Bundeswehr. Proaktives Handeln in der CSO-Rolle wird umso wichtiger: Es ist die **treibende Kraft für Resilienzsteuerung und Lagebildführung**, die über traditionelles reaktives Risikomanagement hinausgehen.

Hybride Bedrohungen sind keine Zukunftsszenarien, sondern tägliche Einsatzlage:

- Mind. 289 Milliarden Euro jährlicher Schaden durch Cyberangriffe, Industriespionage und Sabotage (Bitkom 2025)
- Koordinierte Angriffe auf: Produktionssysteme, Lieferketten, Energieversorgung, Personal, Kommunikation
- Ziele: Destabilisierung, Erpressung, Erosion von Vertrauen und Betriebsfähigkeit
- Akteure: Staatlich gesteuerte APT-Gruppen, hybride Operationen, organisierte Kriminalität

Corporate Security ist die operative Säule der Unternehmensresilienz im Kontext OPLAN DEU:

1. **Vom Objektschutz zur Gesamtverteidigungsarchitektur**
    - Integration in nationale Sicherheitsstrukturen (ZMZ, BSI, CERT-Bund, BBK)
    - Operative Schnittstelle zu Bundeswehr, Nachrichtendiensten und Behörden
    - Teilnahme an behördlichen Lagebesprechungen und Krisenübungen
2. **Von reaktiv zu antizipativ**
    - Aufbau eines integrierten Frühwarnsystems (Security Intelligence Hub)
    - 24/7-Lagebildführung über alle Bedrohungsdimensionen
    - Proaktive Bedrohungsanalyse statt Incident Response
3. **Von Silo zu Integration**
    - Verzahnung mit IT-Security, HR, Supply Chain, Facility, Legal, Communications
    - Mitglied des Resilience Steering Committee auf Vorstandsebene
    - Direkte Berichtslinie zu CEO/CRO

Strategische Handlungsfelder

1. Energie & Rohstoffversorgung

- Absicherung kritischer Energieinfrastruktur (Trafostationen, Notstromsysteme, Tankanlagen)
- Cyber- und physische Härtung von OT-Systemen und Energieleitstellen
- Koordination mit BNetzA und Energieversorgern bei Priorisierungen
- Aufbau dezentraler Eigenversorgung (PV, Batterien, Diesel-Reserven)

2. Lieferketten & Logistik

- Risikotransparenz über gesamte Supply Chain (Tier-1 bis Tier-n)
- Absicherung logistischer IT-Systeme (ERP, Tracking, Port-Management)
- Physischer Schutz kritischer Umschlagplätze und Transportrouten
- Entwicklung dynamischer Risiko-Heatmaps und Dual-Sourcing-Strategien

3. Interne Infrastruktur & Standorte

- Standortklassifizierung nach KRITIS-Definition (DIN SPEC 14027)
- Verstärkung von Zutritts-, Perimeter- und Drohnenschutzsystemen
- Aufbau von Ausweichstandorten ("Hot Sites")
- Einsatz von Sensorik, Drohnenerkennung und OSINT-Monitoring

4. Cyber, Kommunikations- und Betriebssysteme

- Absicherung kritischer IT-, OT- und Kommunikationssysteme
- Aufbau redundanter und segmentierter Netzwerkstrukturen (Zero Trust)
- Einführung autarker Kommunikationssysteme (Satellit, Out-of-Band)
- 24-h-Meldepflicht nach NIS2 bei Sicherheitsvorfällen
- Direkte Kommunikationskanäle zu BSI, CERT-Bund, NATO-Cyber

5. Personal & Arbeitsfähigkeit

- Transparenz über Reservistenstatus und Zivilschutzpflichten (DSGVO-konform)
- Sicherstellung der Mindestbesetzung in kritischen Prozessen
- Schutz der Belegschaft vor physischen und psychischen Bedrohungen
- Cross-Training, Stellvertretermodelle und Employee Assistance Programs

6. Produkte und Dienstleistungen

- Bewertung des Portfolios nach Systemrelevanz und Dual-Use-Potential
- Schutz sicherheitsrelevanter Produktionsdaten und Entwicklungen
- Dual-Use-Compliance nach EU-VO 2021/821
- Absicherung verteidigungsrelevanter Fertigungslinien

7. Recht & Governance

- Sicherstellung der Compliance mit Sicherstellungsgesetzen
- Verankerung von Resilienz in Corporate Policies
- Klärung von Haftungsfragen bei staatlicher Inanspruchnahme
- Erweiterung von Versicherungspolicen (Krieg, Terror, Cyber)

8. Technologie & Innovation

- Schutz geistigen Eigentums und kritischer Entwicklungsdaten
- Absicherung von Forschungseinrichtungen gegen Spionage
- Bewertung von Dual-Use-Technologien
- Integration von ITAR/EAR-Konformität und IP-Security

9. Internationale Verflechtungen & Geopolitik

- Geopolitisches Risikomanagement für alle internationalen Standorte
- Schutz ausländischer Assets vor staatlichen Zugriffen
- Sanktions- und Exportkontroll-Compliance
- Nutzung von Regierungs- und Nachrichtendienst-Lagebildern

10. Märkte & Kundenverhalten

- Monitoring geopolitischer, regulatorischer und sozialer Trends
- Früherkennung von Reputationsrisiken durch hybride Einflussoperationen

- Schutz vor Desinformationskampagnen
- Social-Media-Monitoring und OSINT-Integration

11. Länder- und Standortperspektive

- Harmonisierung sicherheitsrelevanter Standards über alle internationalen Standorte
- Aufbau einer zentralen, international abgestimmten Sicherheits-Governance
- Rechts- und Compliance-Monitoring nationaler Sicherheitsgesetze
- Länderübergreifende Krisenübungen

12. Finanzen & Liquidität

- Sicherung der Zahlungsfähigkeit bei Ausfall von Systemen
- Schutz von Finanz-IT und Transaktionsdaten
- Nutzung mehrerer Banken und alternativer Zahlungsdienstleister
- Integration finanzieller Risiken in BCM

Monitoring & Frühwarnsystem: Kernaufgabe des CSO

Aufbau eines Security Intelligence Hub mit vier Komponenten:

1. **Staatliche Informationsschnittstellen**
   - BSI (Cyberwarnungen, CERT-Bund)
   - BMI/BBK (Krisen- und Bevölkerungsschutz)
   - BMVg/ZMZ (Zivil-Militärische Zusammenarbeit)
   - AA-Krisenzentrum/EU INTCEN (geopolitische Lagebilder)
2. **Private Intelligence-Dienste**
   - Cyber Threat Intelligence, OSINT, Satellitendaten, geopolitische Analysen
3. **Internes Lagebild**
   - IT-Sicherheit, Werkschutz, Lieferketten, Personal, Facility Management
4. **Frühwarnindikatoren (KPIs)**
   - Lieferverzögerungen, Cyber-Anomalien, regionale Eskalationen, Energieverfügbarkeit

Krisenkommunikation: Security als Informations-Hub

- Sicherung der Informationshoheit
- One-Voice-Policy sicherstellen
- Desinformationsabwehr
- Social-Media-Monitoring gegen manipulative Inhalte
- Einbindung in MoWaS (Modulares Warnsystem)

Die Rolle des CSO

- Strategische und operative Führungskraft im nationalen Resilienzverbund
- Koordinator zwischen Unternehmen, Behörden und Bundeswehr
- Lagebildverantwortlicher für alle sicherheitsrelevanten Dimensionen
- Entscheidungsvorbereiter für zeitkritische Maßnahmen
- Schnittstelle zu staatlichen Krisenstäben und ZMZ-Strukturen

Verpflichtungen: Schutz kritischer Standorte, Aufrechterhaltung der Kommunikationsfähigkeit, Koordination mit Sicherheitskräften, Umsetzung staatlicher Weisungen nach ASG

In der hybriden Bedrohungslage entscheidet die Qualität der Sicherheitsarbeit über Betriebskontinuität, Mitarbeitersicherheit, Reputationsschutz, finanzielle Stabilität, rechtliche Compliance und nationale Handlungsfähigkeit.

Fazit:

Corporate Security ist die operative und strategische Säule der Unternehmensresilienz sowie die Schnittstelle zur gesamtstaatlichen Sicherheitsarchitektur.

Vollständiges Whitepaper unter

Herausgeber

ThinkTank Corporate Resilience: *Wo Wirtschaft und Wissenschaft vorausdenken*

Der **ThinkTank Corporate Resilience** schafft eine Plattform, auf der strategische Trends, geopolitische Analysen und Zukunftsszenarien aus der Resilienzperspektive von Chief Security Officers mit der Business-Sicht von CEOs, Vorständen, Aufsichtsräten und Anteilseignern zusammengeführt werden. Er ist aus der engen Zusammenarbeit zwischen Wirtschaft und Wissenschaft an der Technischen Hochschule Ingolstadt im Bereich „Wertschöpfung durch Corporate Security“ entstanden und eng mit dem MBA-Programm **Strategy, Global Risk & Security Management** verbunden.

Initiiert wurde der ThinkTank von Sven Dawson, Florian Haacke, Alexander Klotz, Marco Mille, Johannes Strümpfel und Prof. Dr. Marc Knoppe, um C-Suite-Vertreter, Chief Security Officers und Behörden ein Forum für zukunftsorientiertes Denken sowie den strategischen Austausch über systemische Risiken **aus wirtschaftlicher Sicht** zu bieten.

in Kooperation mit dem

VSW-Bundesverband und dem

Beirat MBA Strategy, Global Risk & Security Management der Technische Hochschule Ingolstadt.

FAQ & Feedback zum Whitepaper

Die Herausforderungen hybrider Kriegsführung betreffen uns alle:
Wirtschaft, Wissenschaft und Gesellschaft. Um gemeinsam tragfähige Lösungen zu entwickeln, möchten wir Ihre Perspektive einbeziehen.

Haben Sie Fragen oder Anregungen?

Nutzen Sie unseren Feedback-Fragebogen oder kontaktieren Sie direkt unseren Thinktank. Ihre Impulse sind wertvoll und können entscheidend dazu beitragen, zukünftige Veröffentlichungen noch praxisnäher und relevanter zu gestalten.

Besuchen Sie unsere FAQs, um Antworten auf häufige Fragen zu erhalten und sich tiefer in das Thema einzuarbeiten.

👉 **Kontakt & Feedback**

VSW
Bundesverband

LEAD.SECURE.SHAPE RESILIENCE
THI
MBA STRATEGY, GLOBAL RISK AND SECURITY MANAGEMENT