

Mehr als Regulierung – KRITIS Dachgesetz ist Paradigmenwechsel

Resilienz als Teil der Unternehmensführung systematisch verankert

BIM-MAGAZIN: Sehr geehrter Herr Gerstenberg, für den notwendigen Schutz vor Cyber-Kriminalität gibt es seit Jahren eine hohe Sensibilität in Wirtschaft und öffentlicher Verwaltung. Mit der Umsetzung der EU-CER-Richtlinie im KRITIS-Dachgesetz geht es nun aber auch um die physische Sicherheit und Notfallvorsorge. Wer ist betroffen und um welche Maßnahmen geht es?

Uwe Gerstenberg: Mit dem KRITIS-Dachgesetz erweitert sich der regulatorische Fokus deutlich: Neben der Cyber-Resilienz rückt nun die physische Sicherheit gleichrangig in den Mittelpunkt.

Betroffen sind organisationsübergreifend Betreiber sogenannter kritischer Einrichtungen – dazu zählen unter anderem Energieversorger, Krankenhäuser, Wasser- und Abfallwirtschaft, Verkehrs- und Logistikunternehmen sowie Teile der öffentlichen Verwaltung. Insgesamt spricht man von über 40.000 Organisationen in Deutschland.

Im Kern verpflichtet das Gesetz diese Betreiber, Resilienzsysteme aufzubauen, die sowohl präventiv als auch reaktiv wirken.

Dazu gehören insbesondere:

- » Risiko- und Bedrohungsanalysen (auch auf physische Angriffe)
- » Schutzkonzepte für Anlagen und Personal
- » Notfall- und Krisenmanagementstrukturen
- » Übungen und Szenario-Planungen (z. B. Sabotage, Blackout, hybride Bedrohungen)
- » sowie Melde- und Kommunikationsprozesse.

Neu ist die klare Erwartung, dass Organisationen ihre Resilienz ganzheitlich („integrale Sicherheit“) und nicht mehr silohaft aufstellen.

Uwe Gerstenberg

99

Neu ist die klare Erwartung, dass Organisationen ihre Resilienz ganzheitlich („integrale Sicherheit“) und nicht mehr silohaft aufstellen.“

BIM-MAGAZIN: Sind davon private Organisationen ebenso betroffen, wie öffentliche Verwaltungen? Und wer trägt aus rechtlicher Perspektive die Verantwortung?

Uwe Gerstenberg: Ja – das ist eine der zentralen Veränderungen. Anders als früher betrifft der Rechtsrahmen nicht nur klassische staatliche Einrichtungen, sondern ausdrücklich auch private Betreiber kritischer Dienstleistungen. Die Verantwortung liegt rechtlich klar auf Führungsebene, insbesondere bei der Geschäftsleitung beziehungsweise den verantwortlichen Organen.

Diese haben eine Organisationspflicht zur Risikovorsorge. Verstöße können haftungsrechtliche Konsequenzen haben – insbesondere dann, wenn Schäden durch unzureichende Vorbereitung entstehen.

Gleichzeitig beobachten wir eine Verschiebung: Verantwortung wird zunehmend nicht nur juristisch, sondern auch operativ überprüfbar gemacht. Dokumentation, Nachweisfähigkeit und Auditierbarkeit gewinnen daher massiv an Bedeutung.

BIM-MAGAZIN: Müssen die Verantwortlichen alle genannten Maßnahmen zwingend umsetzen oder bestehen Interpretationsspielräume?

Uwe Gerstenberg: Das Gesetz formuliert bewusst risikobasierte und verhältnismäßige Anforderungen. Es gibt also keinen starren Maßnahmenkatalog, sondern einen Rahmen, der organisationsindividuell ausgestaltet werden muss.

Das führt zu einem gewissen Interpretationsspielraum – allerdings mit einer klaren Einschränkung: Dieser Spielraum endet dort, wo Risiken objektiv erkennbar sind und keine angemessenen Maßnahmen getroffen wurden.

In der Praxis müssen Organisationen nachweisen können, dass sie

1. ihre Risiken systematisch analysiert haben
2. geeignete Schutzmaßnahmen definiert haben und
3. diese auch implementiert und regelmäßig überprüft werden.

Der Maßstab ist dabei nicht „Perfektion“, sondern angemessene Resilienzfähigkeit im Verhältnis zum Risiko.



Uwe Gerstenberg ist Sicherheitsexperte, Unternehmer sowie Managing Director der Luther Public Service GmbH. Nach beruflichen Stationen im staatlichen Sicherheitsumfeld berät er seit vielen Jahren Unternehmen, KRITIS-Betreiber und öffentliche Einrichtungen zu integraler Sicherheit, Risiko- und Krisenmanagement. Er gilt als Vordenker für „vireale Sicherheit“ – die Verbindung von physischer und digitaler Resilienz.



Zur Luther Public Services:

Luther Public Services GmbH ist die spezialisierte Beratungseinheit der Luther Rechtsanwaltsgesellschaft für den öffentlichen Sektor und KRITIS-Betreiber. Das Unternehmen unterstützt Behörden, öffentliche Einrichtungen und sicherheitsrelevante Organisationen unter anderem bei der Umsetzung von Resilienz-, Sicherheits- und Compliance-Anforderungen. Der Fokus liegt auf integralen Sicherheitskonzepten, Risiko- und Krisenmanagement sowie der rechtskonformen Umsetzung regulatorischer Vorgaben – insbesondere im Kontext kritischer Infrastrukturen und hybrider Bedrohungslagen.



BIM-MAGAZIN: *Blicken wir auf die Fähigkeit zur Kommunikation – insbesondere bei einem Blackout. Spricht das KRITIS-Dachgesetz hier von einer Pflicht?*

Uwe Gerstenberg: Ja – Kommunikation ist ein zentrales Element der Resilienz Anforderungen, auch wenn sie nicht immer explizit als Einzelpflicht formuliert ist.

Konkret geht es um zwei Ebenen:

Interne Kommunikationsfähigkeit, um Führung und Betrieb aufrechtzuerhalten, sowie externe Kommunikation, insbesondere Meldekettensystemen gegenüber Behörden und Partnern.

Bei Szenarien wie einem Blackout wird deutlich: Standardkommunikation (Mobilfunk, Internet) fällt oft aus.

Daraus ergibt sich faktisch die Pflicht, redundante und resiliente Kommunikationslösungen vorzuhalten, etwa:

- » Satellitenkommunikation,
- » analoge Rückfallsysteme,
- » Notfallinformationsketten (z. B. über Leitstellen).

Unterlassene Vorbereitung kann im Ernstfall als Organisationsverschulden bewertet werden.

BIM-MAGAZIN: *Wie sollen die Betroffenen die Pflichten einhalten, wenn es technisch oder finanziell schwierig ist – etwa bei längeren Blackouts oder begrenzten Budgets?*

Uwe Gerstenberg: Das ist eine realistische und häufige Frage aus der Praxis. Das Gesetz verlangt keine unrealistischen Lösungen, sondern angemessene Vorsorge im Rahmen der Möglichkeiten. Wichtig ist dabei: Es wird nicht verlangt, dass jedes Szenario vollständig beherrscht wird, wohl aber, dass Organisationen sich ernsthaft vorbereiten und priorisieren.

Ich empfehle hier einen risikobasierten Ansatz mit Priorisierung:

- » Welche Funktionen sind kritisch?
- » Welche Ausfallzeiten sind tolerierbar?
- » Welche Minimalfähigkeit muss zwingend erhalten bleiben?

Darauf aufbauend werden Maßnahmen abgestuft umgesetzt. Ergänzend sollten Kooperationsmodelle genutzt werden – etwa mit Behörden, Dienstleistern oder Branchenlösungen.

Förderprogramme und politische Unterstützung werden perspektivisch eine größere Rolle spielen, sind aber derzeit noch nicht flächendeckend etabliert.

BIM-MAGAZIN: *Welche Vorgehensweise empfehlen Sie, um mit der eigenen Organisation Rechtskonformität zu erzielen?*

Uwe Gerstenberg: Der Schlüssel liegt in einem strukturierten, pragmatischen Vorgehen. Ich empfehle ein fünfstufiges Modell:

1. Lagebild & Betroffenheitsanalyse

Klärung, ob und in welchem Umfang die Organisation unter das KRITIS-Dachgesetz fällt.

2. Risiko- und Szenarioanalyse

Identifikation von relevanter Gefährdungen – von Sabotage über Naturereignisse bis zum Blackout oder hybriden Angriff.

3. Resilienzstrategie entwickeln

Definition von Schutzmaßnahmen, Notfallorganisation und Krisenstrukturen.

4. Umsetzung & Integration

Verankerung in Prozesse, Verantwortlichkeiten und Organisation (inkl. Schulungen und Übungen) Nachweisfähigkeit & kontinuierliche Verbesserung

5. Dokumentation, Auditfähigkeit und regelmäßige Aktualisierung.

Entscheidend ist: Resilienz darf kein einmaliges Projekt sein, sondern muss als Teil der Unternehmensführung systematisch verankert werden.

BIM-MAGAZIN: *Ihr Fazit?*

Uwe Gerstenberg: Das KRITIS-Dachgesetz ist mehr als Regulierung – es ist ein Paradigmenwechsel. Organisationen müssen Sicherheit künftig als strategischen Bestandteil ihrer Leistungsfähigkeit begreifen. Wer frühzeitig investiert – in Resilienz, Strukturen und Szenarienkompetenz – wird nicht nur rechtskonform handeln, sondern auch operativ stabiler und wettbewerbsfähiger sein.

Uwe Gerstenberg

99

Verantwortung wird nicht nur juristisch, sondern auch operativ überprüfbar gemacht. Dokumentation, Nachweisfähigkeit und Auditierbarkeit gewinnen daher massiv an Bedeutung.“

Weiterführende Links:

🔗 [Luther Public Services](#)