3

EISENMENGER (Hrsg.)

Schriftenreihe des Forschungsinstituts für Unternehmenssicherheit und Sicherheitswirtschaft (FORSI)

FORSI-Jahresband 2023

Der Schutz Kritischer Infrastrukturen

Neuregelungen zum Einsatz Künstlicher Intelligenz und Drohnen

Akademie der POLIZEI Hamburg

FORSI
Forschungsinstitut für Unternehmenssicherheit und Sicherheitswirtschaft

BOORBERG

FORSI-Jahresband 2023

Der Schutz Kritischer Infrastrukturen (KRITIS)

Neuregelungen zum Einsatz Künstlicher Intelligenz und Drohnen

herausgegeben von

Prof. Dr. Sven Eisenmenger
Hochschule der Akademie der Polizei Hamburg,
Leiter des Forschungsinstituts für Unternehmenssicherheit
und Sicherheitswirtschaft (FORSI)

BOORBERG

Bibliografische Information der Deutschen Nationalbibliothek | Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.

ISBN 978-3-415-07608-2

Satz: Olaf Mangold Text & Typo, 70374 Stuttgart | Druck und Bindung: Laupp & Göbel GmbH, Robert-Bosch-Straße 42, 72810 Gomaringen

Richard Boorberg Verlag GmbH & Co KG | Scharrstraße 2 | 70563 Stuttgart
Stuttgart | München | Hannover | Berlin | Weimar | Dresden
www.boorberg.de

Grußwort anlässlich der 3. FORSI-Sicherheitstagung

Prof. Dr. Sven Eisenmenger

Herzlich willkommen, meine Damen und Herren, herzlich willkommen in der Hochschule der Akademie der Polizei Hamburg und beim FORSI!

Der Schutz Kritischer Infrastrukturen (KRITIS) –
unter Berücksichtigung des neuen Rechtsrahmens für Staat,
KRITIS-Betreiber und Sicherheitswirtschaft

So lautet unser Thema der heutigen Tagung und der volle Saal belegt: Es handelt sich um ein hochaktuelles Thema!

Die Auswirkungen des Ukraine-Krieges und Sabotageakte (Schienennetz, Ostsee-Gaspipeline) ebenso wie die Pandemie haben deutlich gemacht, wie anfällig Kritische Infrastrukturen sind. Der Klimawandel und Naturkatastrophen kommen als Risikofaktoren hinzu.

Die neu geschaffene CER-Richtlinie oder Resilienz-Richtlinie legt Mindeststandards für die staatliche Überwachung und für KRITIS-Betreiber fest, die in nationales Recht umzusetzen sind. Die Umsetzung in Deutschland wird in dem geplanten „KRITIS-Dachgesetz" erfolgen. Erstmals soll ein rechtlicher Gesamtrahmen für Kritische Infrastrukturen geschaffen werden. Betroffen von den Regelungen sind perspektivisch Behörden und aus dem Unternehmensbereich KRITIS-Betreiber. Von großem Interesse in der Praxis und diskutiert ist auch die Frage der Berücksichtigung der Sicherheitswirtschaft in dem KRITIS-Dachgesetz.

Mit der CER-Richtlinie und dem Entwurf des KRITIS-Dachgesetzes – also mit dem physischen Schutz – möchten wir uns befassen, aber auch in einem eigenen Teil mit der Cybersicherheit, denn hier liegen bereits Regulierungserfahrungen vor und diese Erfahrungen sollte man auch in der KRITIS-Dachgesetz-Debatte fruchtbar machen, abgesehen davon, dass auch in der Cybersicherheit eine Neuregelung ansteht.

Zum Ablauf:

Der anschließende 2. Teil „Grundlagenteil und Rechtsrahmen" bezieht sich im Schwerpunkt auf den physischen Schutz, damit auf die CER-Richtlinie, auf das KRITIS-Dachgesetz und ein Resilienzmodell. Wir hören dazu zunächst das Referat von Herrn *Alexander Frank*, Head of EU Affairs, Confederation of European Security Services (CoESS), der sich mit der CER-Richtlinie befassen wird („Bericht aus Brüssel"). Anschließend möchte ich

Ihnen den KRITIS-Dachgesetz-Entwurf vorstellen und dabei auch auf die Rolle der Sicherheitswirtschaft eingehen. *Prof. Dr. André Röhl*, NBS Northern Business School, wird sich schließlich eingehend mit dem Begriff „Resilienz" befassen, ein Resilienzmodell vorstellen und den Grundlagenteil damit abrunden. Anschließend besteht Gelegenheit zur Diskussion. Dieser Teil wird von *Prof. Dr. Dr. h. c. mult. Rolf Stober*, Universität Hamburg, moderiert, der auch gleich übernehmen wird.

Der 3. Teil befasst sich mit dem Schutz Kritischer Infrastrukturen aus dem Blickwinkel des Staates und dies verbinden wir mit dem Referenzgebiet Cybersicherheit, weil hier Regulierungserfahrungen auf allen Seiten aus der Vergangenheit vorliegen, die man in der aktuellen Diskussion sicher gebrauchen kann. Abgesehen davon wird auch der Cybersicherheitsrahmen derzeit novelliert. Wir freuen uns sehr auf die Erfahrungsberichte von Frau *Anja Wells*, Referat WG 11 – KRITIS-Grundsatz, Bundesamt für Sicherheit in der Informationstechnik (BSI), und von Herrn *Andreas Dondera*, LKA 54, Polizei Hamburg. Die Diskussion erfolgt unter der Leitung von Herrn wiss. Mitarbeiter *Nils Pohl*, FORSI.

Nach der Mittagspause steht dann im 4. Teil der Schutz Kritischer Infrastrukturen aus dem Blickwinkel von KRITIS-Betreibern und Sicherheitswirtschaft im Vordergrund (Praxisteil). Dieser Teil wird sich mit dem physischen Schutz und sicher am Rand auch mit der Cybersicherheit befassen. Hier sind wir gespannt auf den Beitrag zum Energiesektor von *Nils Retkowski*, Referent Unternehmenssicherheit, HanseWerk AG, sowie zur Sicherheitswirtschaft von *Jens Müller*, Geschäftsführer/Chief Public Affairs, Securitas Holding GmbH, und Vizepräsident des BDSW. Geleitet wird die Diskussion von *Prof. Dr. Harald Olschok*, Hochschule für Wirtschaft und Recht Berlin.

Meine Damen und Herren, das FORSI ist seit 2021 an der Hochschule der Akademie der Polizei Hamburg eingerichtet und wir werden uns auch 2024 den aktuellen Themen der Sicherheitswirtschaft und der Unternehmenssicherheit in Form von Tagungen, Expertenworkshops und Publikationen widmen. Dazu halten wir Sie auf dem Laufenden.

Ich danke Ihnen für Ihre Teilnahme, den genannten Mitwirkenden für Ihren Beitrag und im Bereich der Organisation geht ein großer Dank an *Hannah van Elsbergen* und *Nils Pohl*, *Peter Hagemann* und *Nick Bollhorst*.

Meine Damen und Herren: wir fangen an!

Der Entwurf des KRITIS-Dachgesetzes: Ein Rechtsrahmen mit offenen Flanken

Prof. Dr. Dr. h. c. mult. Rolf Stober

Staatliches und privates Handeln setzen die Existenz, Unterhaltung und Weiterentwicklung einer ökonomischen, sozialen, ökologischen, technischen und digitalen Infrastruktur voraus. Zu Recht spricht das Bundesverfassungsgericht bei diesen Daseins- und Zukunftsvorsorgeaufgaben von einem Infrastruktursicherungsauftrag[1].

Dieser Auftrag verdichtet sich, wenn Kritische Infrastrukturen vor Bedrohungen, Gefährdungen und Störungen geschützt werden sollen. Dabei geht es um nichts weniger als um die reibungslose Aufrechterhaltung wesentlicher Funktionen zur kontinuierlichen Bewältigung alltäglicher Herausforderungen für Staat und Selbstverwaltung, Gesellschaft und Wirtschaft (§ 1 E-KRITIS-Dachgesetz).

Infrastruktursicherung tangiert deshalb auch die Grundrechte, weil ihre Gewährleistung unabdingbar für die uneingeschränkte Wahrnehmung von Freiheitsrechten ist. Dieser Anspruch gilt nicht nur für die lebenden Generationen. Er erfasst, wie das Bundesverfassungsgericht im sog. Klimabeschluss herausgearbeitet hat, auch künftige Generationen. Sie sollen ebenfalls die Chance haben, an heute vorhandenen Kritischen Infrastrukturen zu partizipieren[2].

Dieser verfassungsrechtlich verbürgte Schutz gelingt nur, wenn die als kritisch identifizierten Einrichtungen und Dienste resilient sind. Angesichts unsicherer Zeiten und permanent wechselnder Lagebilder ist der auf dem All-Gefahren-Ansatz basierende Schutz Kritischer Infrastrukturen ein zentrales politisches, ökonomisches und juristisches Kernthema[3], das unter der Überschrift „Krisenschutz der Daseinsvorsorge" auch Gegenstand eines Gesprächskreises bei der im Oktober 2023 stattfindenden Staatsrechtslehrertagung in Bochum ist.

Als Referenz für den Tagungsort mögen zwei Hamburger Beispiele die aktuelle Relevanz der damit verbundenen Probleme beleuchten:

---

1 BVerfGE 108, 370, 393.

2 BVerfG, NJW 2021, 1723 ff.

3 S. schon G. *Hünnekens*, Rechtsfragen der wirtschaftlichen Infrastruktur, 1995; *Stober* in Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, 2010, 121 ff.; *Guckelberger*, DVBl. 2019, 525 ff.; *Stober/Korte*, Öffentliches Wirtschaftsrecht, Allgemeiner Teil, 20. Aufl. 2023, § 26; RL EU 2022/2557 v. 14.12.2022 zur IT-Sicherheit Kritischer Infrastrukturen.

– Die außenwirtschaftlich motivierte Diskussion um die Beteiligung der chinesischen Staatsreederei COSCO an dem Hamburger Hafen-Terminal Tollerort im Frühjahr 2023.
– Die umweltpolitisch angelegte Debatte um die Klimakleber-Aktion im Hamburger Flughafen am 13. Juli 2023.

Diese exemplarische Auswahl belegt, dass der Schutz Kritischer Infrastrukturen ein hohes dreidimensional ausgerichtetes Gut ist:
– Er ist ein individuelles privates Gut.
– Er ist ein kollektives gesellschaftliches Gut.
– Er ist ein staatliches und binnenmarktgeprägtes öffentliches Gut.

Diese Kategorisierung bedeutet, dass der Schutz kritischer Einrichtungen weder nur in der Eigenverantwortung des Einzelnen liegen noch allein vom Staat oder einem Staatsverbund geleistet werden kann. Vielmehr besteht eine Mit- und Gesamtverantwortung darin, dass sich sämtliche Akteure an dieser Aufgabe beteiligen und effizient zusammenwirken.

Die jüngere Vergangenheit hat gezeigt: Europa und Deutschland, Gesellschaft und Wirtschaft, Unternehmen und Konsumenten, Unternehmenssicherheit und Sicherheitswirtschaft sind resilient und können kritische infrastrukturelle Situationen meistern. Man denke nur an die
– Finanzkrise,
– Terrorismuskrise,
– Coronakrise oder an die
– Energiekrise.

Hingegen steht die Bewältigung weiterer Krisen aus. Hier setzt das Thema der Tagung an, die sich aus unterschiedlichen Richtungen dem Schutz Kritischer Infrastrukturen widmet.

Der erste Hauptteil der Veranstaltung konzentriert sich auf die EU-Richtlinie 2022/2557 über die Resilienz Kritischer Infrastrukturen (sog. CER-Richtlinie)[4] sowie deren Umsetzung in nationales Recht durch das sog. KRITIS-Dachgesetz.

Ausweislich der Erwägungsgrunde und der sie konkretisierenden Einzelbestimmungen verfolgen die CER-Richtlinie im Rahmen einer angestrebten Mindestharmonisierung (Erwägungsgründe 1 und 3) und der Entwurf des-KRITIS-Dachgesetzes folgende Zwecke:
– Festlegung strategischer Ziele und Maßnahmen zum Schutz kritischer Einrichtungen (Art. 4 E-KRITIS-Dachgesetz).

4 Die Richtlinie klammert die Aspekte IT- und Cybersicherheit aus (Art. 1 Abs. 2), die Gegenstand der EU-Richtlinie 2022/2055 sind.

– Ermittlung kritischer Einrichtungen anhand eines risikobasierten Ansatzes (Art. 6 Abs. 2 und 17 sowie Erwägungsgründe 15 f. CER-Richtlinie, § 1 E-KRITIS-Dachgesetz).
– Auferlegung von Mindestverpflichtungen für kritische Einrichtungen (Art. 12 ff. CER-Richtlinie und § 1 KRITIS-Dachgesetz) im Sinne eines Risikoplanes und eines Risikomanagements einschließlich Zuverlässigkeitsüberprüfungen (Art. 13 und Erwägung 32 CER-Richtlinie, § 10 ff. E-KRITIS-Dachgesetz).
– Unterstützungsmaßnahmen für kritische Einrichtungen (Art. 1 und Erwägung 25 CER-Richtlinie, § 1 E-KRITIS-Dachgesetz).
– Optimierung von Aufsichts- und Durchsetzungsbefugnissen (Art. 1 und 21 f., Erwägungen 22 ff.; § 1 E-KRITIS-Dachgesetz).
– Verbesserung der Zusammenarbeit zwischen öffentlichen und privaten Infrastrukturträgern (Art. 4 Abs. 2 lit. c CER-Richtlinie)[5].

Zusammenfassend sollen die angesprochenen öffentlichen und privaten Unternehmen so ertüchtigt werden, dass sie bei Bedrohungen umfassend agieren und reagieren können, um Störungen abzuwenden.

Die Referenten erörtern nun den Rechtsrahmen Kritischer Infrastrukturen aus binnenmarktrechtlicher sowie aus nationaler Sicht und präsentieren ein eigenständiges Resilienz-Modell[6].

5 S. dazu Stober/Eisenmenger/Olschok (Hrsg.), Handbuch Sicherheitswirtschaft und Öffentlich-Private Sicherheitskooperation, 2023.

6 S. dazu auch *A. H. Karsten* in Voßschmidt/Karsten (Hrsg.), Resilienz und kritische Infrastruktur, 2019, 322 ff.

Entstehung, Inhalte und Perspektiven der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)

Alexander Frank

Im Dezember 2022 haben der Europäische Rat und das Parlament die EU-Richtlinie 2022/2557 über die Resilienz kritischer Einrichtungen verabschiedet. Die Richtlinie spiegelt die neue Bedrohungslage wider, mit der Kritische Infrastrukturen in Europa nicht erst seit dem russischen Krieg gegen die Ukraine konfrontiert sind. Mit dem Ziel, den europäischen Binnenmarkt aufgrund der zunehmenden Interdependenz wesentlicher Dienste besser zu schützen, legt sie erstmals einen harmonisierten Rahmen für den Schutz Kritischer Infrastrukturen in ganz Europa fest, um gleiche Wettbewerbsbedingungen und ein ähnliches Schutzniveau in allen EU-Mitgliedstaaten zu gewährleisten. In Anbetracht der Tatsache, dass die innere Sicherheit und der Katastrophenschutz eigentlich zu den Kernkompetenzen der Mitgliedstaaten gehören, ist die Richtlinie ein echter Meilenstein – auch für die Sicherheitswirtschaft, wenn diese nun konsequent auf nationaler Ebene, in Deutschland durch das KRITIS-Dachgesetz, umgesetzt wird.

I. Entstehung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)

Die EU-Richtlinie 2022/2557 über die Resilienz kritischer Einrichtungen, die im Dezember 2022 von den EU-Institutionen in Brüssel verabschiedet wurde, wird derzeit in Deutschland durch das KRITIS-Dachgesetz in nationales Recht umgesetzt. Sie ist das Ergebnis politischer, wirtschaftlicher und gesellschaftlicher Entwicklungen, die zu der Notwendigkeit geführt haben, den Rechtsrahmen für den Schutz Kritischer Infrastrukturen auf europäischer Ebene zu stärken.

Zunächst zum politischen Hintergrund: In erster Linie handelt es sich bei der neuen Richtlinie um eine Überarbeitung der Richtlinie 2008/114 über die Ermittlung und Ausweisung Europäischer Kritischer Infrastrukturen. Aufgrund der begrenzten Zuständigkeiten der EU in Fragen der inneren Sicherheit und des Katastrophenschutzes war die Wirkung der alten Richtlinie sehr begrenzt: Sie deckte nur zwei Sektoren ab (Energie und Verkehr) und legte lediglich einen Rahmen für die Ermittlung sogenannter Kritischer Europäischer Infrastrukturen fest – definiert als Kritische Infrastrukturen,

deren Störung oder Zerstörung erhebliche Auswirkungen auf mindestens zwei Mitgliedstaaten hätte. Sobald diese Infrastrukturen identifiziert wurden, mussten sie einen Sicherheitsplan aufstellen und einen Sicherheitsbeauftragten benennen. Bereits 2018 bezeichnete der Bericht 2018/2044 des Europäischen Parlaments die Richtlinie 2008/114 als veraltet und forderte eine Überarbeitung. Im April 2019 kam die Europäische Kommission selbst zu demselben Schluss:

> „Zehn Jahre nach ihrem Inkrafttreten scheint die Richtlinie heute nur noch teilweise oder gar nicht mehr relevant zu sein, insbesondere in Anbetracht der jüngsten technologischen, wirtschaftlichen, sozialen, politischen und ökologischen Entwicklungen und aktuellen Herausforderungen. Die zunehmende Verflechtung und die gegenseitigen Abhängigkeiten zwischen den Sektoren sowie der grenzüberschreitende Charakter der Bedrohungen und die potenziellen Folgen einer Störung/Zerstörung Kritischer Infrastrukturen zeigen, dass die EU in diesem Politikbereich weiterhin tätig sein muss."

Es wurde daher weitgehend erwartet, dass die Europäische Kommission nach den Europawahlen im Mai 2019 einen Vorschlag für eine überarbeitete Richtlinie vorlegen wird.

Auch wirtschaftlich ergibt die nun verabschiedete CER-Richtlinie Sinn. Bereits im ersten Erwägungsgrund des Gesetzestexts heißt es:

> „In einer zunehmend verflochtenen Unionswirtschaft kommt kritischen Einrichtungen als Anbietern wesentlicher Dienste eine unverzichtbare Rolle bei der Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im Binnenmarkt zu. Daher ist es von wesentlicher Bedeutung, einen Unionsrahmen zu schaffen, der sowohl darauf abzielt, die Resilienz kritischer Einrichtungen im Binnenmarkt durch die Festlegung harmonisierter Mindestverpflichtungen zu verbessern, als auch darauf, diesen Einrichtungen durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu helfen."

Erwägungsgrund 6 der Richtlinie führt weiter fort:

> „Die an der Erbringung wesentlicher Dienste beteiligten Einrichtungen unterliegen zunehmend unterschiedlichen Anforderungen, die sich aus nationalem Recht ergeben. Der Umstand, dass in einigen Mitgliedstaaten weniger strenge Sicherheitsanforderungen für diese Einrichtungen gelten, führt nicht nur zu unterschiedlichen Resilienzniveaus, sondern bringt auch das Risiko negativer Auswirkungen auf die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätig-

keiten in der gesamten Union mit sich und führt ferner auch zu Hindernissen für das reibungslose Funktionieren des Binnenmarkts."

Die Rechtsgrundlage für die EU, rechtsverbindliche Rechtsvorschriften zum Schutz Kritischer Infrastrukturen zu erlassen, die in der Regel eine Kernkompetenz der EU-Mitgliedstaaten sind, ergibt sich insbesondere aus genau diesem Grund: dem Schutz des europäischen Binnenmarkts.

Die zunehmende Verwundbarkeit des europäischen Binnenmarkts hat nicht zuletzt mit einer Veränderung der Gefahrenlage zu tun. Sowohl das Europaparlament als auch die Europäische Kommission verwiesen bereits 2018 und 2019 auf eine wachsende Gefährdung von Kritischer Infrastruktur in Europa, damals insbesondere im Zeichen einer Reihe von Terroranschlägen in den 2010er-Jahren sowie der Zunahme von Cyberattacken. Seitdem ist viel passiert: Die Covid-19 Pandemie und der Krieg Russlands gegen die Ukraine haben uns weiter die Verwundbarkeit Kritischer Infrastrukturen und der durch diese erbrachten wesentlichen Dienste vor Augen geführt.

Die CER-Richtlinie ist gemeinsam mit der EU-Richtlinie 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, kurz genannt „NIS-2-Richtlinie", verabschiedet worden. Beide Richtlinien sind sich in Inhalt und Ansatz sehr ähnlich. Die CER-Richtlinie befasst sich jedoch nur mit der physischen Widerstandsfähigkeit kritischer Einrichtungen, während die NIS-2-Richtlinie einen Rechtsrahmen für deren Cyber-Resilienz schafft.

II. Inhalt der CER-Richtlinie

Die CER-Richtlinie legt ein Verfahren fest, mit dem die EU-Mitgliedstaaten „kritische Einrichtungen" in den folgenden 11 Sektoren ermitteln sollen: Energie, Verkehr, Bankwesen, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Weltraum, sowie Produktion, Verarbeitung und Vertrieb von Lebensmitteln.

Diese Einrichtungen müssen dann laut Art. 13 der Richtlinie geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen ergreifen, um ihre Widerstandsfähigkeit gegenüber physischen Gefahren zu gewährleisten – und darüber berichterstatten.

Ganz konkret legt die Richtlinie folgende Schritte fest:

1. Bis Januar 2026 müssen die EU-Mitgliedstaaten eine nationale Resilienzstrategie verabschieden – und aktualisieren diese mindestens alle vier Jahre.
Diese Strategie sollte klare strategische Ziele für die Resilienz kritischer Einrichtungen sowie einen Rahmen für deren Umsetzung setzen, einschließlich einer Beschreibung der Aufgaben und Zuständigkeiten der jeweiligen Behörden, kritischen Einrichtungen und sonstigen an der Umsetzung der Strategie beteiligten Akteure. Weiter sollen das Verfahren, nach dem kritische Einrichtungen anhand der Vorgaben der EU-Richtlinie identifiziert werden (siehe Punkt 2), sowie die Maßnahmen dargelegt werden, die diese basierend auf Art. 13 der EU-Richtlinie in die Wege leiten müssen (siehe Punkt 3). Auch sollte die Strategie erklären, wie Betreiber kritischer Einrichtungen bei der Umsetzung der gesetzlich erforderlichen Maßnahmen unterstützt werden sollen.

2. Ebenfalls bis Januar 2026 führt jeder Mitgliedstaat eine Risikobewertung in den 11 Sektoren durch und ermittelt dabei „kritische Einrichtungen".
Dies findet anhand eines in Art. 5 beschriebenen Risikobewertungsverfahrens sowie folgender Kriterien statt: (1) Die Einrichtung ist im Mitgliedstaat tätig und ansässig, (2) die Einrichtung erbringt einen oder mehrere „wesentliche Dienste" und (3) ein Sicherheitsvorfall würde eine „erhebliche Störung" bei der Erbringung eines/mehrerer wesentlicher Dienste bewirken.

Ein „wesentlicher Dienst" wird in Art. 2 der Richtlinie definiert als „Dienst, der für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder der Erhaltung der Umwelt von entscheidender Bedeutung ist". Die Liste an wesentlichen Diensten in den 11 Sektoren, die in den Anwendungsbereich der Richtlinie fallen, wurde erst kürzlich die die Europäische Kommission in einer delegierten Rechtsakte vom 25. Juli 2023 weiter definiert.

Der Begriff „erhebliche Störung" ist weiter in Art. 7 definiert und hängt beispielsweise von Anzahl und Anteil betroffener Nutzer, dem Marktanteil des Dienstes, der Dauer der Störung, Abhängigkeiten mit anderen wesentlichen Diensten sowie dem betroffenen geografischen Gebiet der Störung ab.

Die Risikobewertung und die damit einhergehende Identifizierung kritischer Einrichtungen müssen mindestens alle vier Jahre durchgeführt werden.

3. Kritische Einrichtungen müssen Resilienzmaßnahmen in die Wege leiten.

Bis zum 17. Juli 2026 ermittelt jeder Mitgliedstaat die kritischen Einrichtungen für die in den Anwendungsbereich fallenden Sektoren und wesentlichen Dienste, und informiert diese innerhalb eines Monats. Die Betreiber kritischer Einrichtungen haben anschließend 9 Monate Zeit, um eine eigene Risikobewertung nach Art. 12 vorzunehmen sowie um geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu ergreifen, die erforderlich sind, um

– Sicherheitsvorfälle zu verhindern,
– einen angemessenen physischen Schutz zu gewährleisten,
– Sicherheitsvorfälle abzuwehren und Folgen zu begrenzen,
– eine Wiederherstellung der Dienste zu gewährleisten und
– das Personal für die Maßnahmen zu sensibilisieren.

Für die Sicherheitswirtschaft ist insbesondere Art. 13 Abs. 1 lit. e relevant. Dieser fordert von Betreibern, „ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten".

Laut Art. 16 fördern die Mitgliedstaaten die Anwendung von europäischen und internationalen Normen und technischen Spezifikationen, um Betreiber kritischer Einrichtungen bei der Umsetzung dieser Maßnahmen zu unterstützen.

Die getätigten Maßnahmen müssen Betreiber kritischer Einrichtungen in einem Resilienzplan zusammenfassen und den Behörden zur Verfügung stellen.

4. Die Meldung von Sicherheitsvorfällen ist geregelt.

Laut Art. 15 sollen kritische Einrichtungen der zuständigen Behörde Sicherheitsvorfälle, die die Erbringung wesentlicher Dienste erheblich stören oder stören könnten, unverzüglich und innerhalb von 24 Stunden melden, gegebenenfalls gefolgt von einem ausführlichen Bericht spätestens einen Monat danach.

Hat ein Sicherheitsvorfall erhebliche Auswirkungen auf die Kontinuität der Erbringung wesentlicher Dienste für oder in sechs oder mehr Mitgliedstaaten oder könnte er solche Auswirkungen haben, so melden die zuständigen Behörden der vom Sicherheitsvorfall betroffenen Mitgliedstaaten diesen Sicherheitsvorfall der Kommission.

III. Relevanz der Richtlinie für die Sicherheitswirtschaft

Wie erwähnt ist insbesondere Art. 13 Abs. 1 lit. e, der Betreibern kritischer Einrichtungen Maßnahmen zum Personal-Sicherheitsmanagement empfiehlt, für die Sicherheitswirtschaft äußerst interessant.

Denn Sicherheitsunternehmen und -personal sind in vielen Ländern ein integraler Bestandteil des Schutzes Kritischer Infrastrukturen und entsprechender Maßnahmen. Gerade beim Schutz Kritischer Infrastrukturen müssen Sicherheitsdienstleistungen höchsten Qualitätsansprüchen genügen. Dies spiegelt sich jedoch bisher oft nicht in der Beschaffungspraxis der Betreiber wider – ein Problem, auf das die CoESS, gemeinsam mit unserem Sozialpartner UNI Europa, seit Jahren hinweist. Es sollte beispielsweise selbstverständlich sein, dass Behörden und Betreiber ausschließlich Sicherheitsunternehmen mit ausreichend geschultem, ausgerüstetem und qualifiziertem Sicherheitspersonal einsetzen, um diese für das Funktionieren unserer Gesellschaften und Volkswirtschaften wichtigen Einrichtungen zu schützen.

Die CER-Richtlinie setzt in den Art. 13 und 16 genau hier an: Es ist das erste EU-Gesetz, das eine Qualitätskontrolle von kritischem Personal im Bereich des Schutzes kritischer Infrastrukturen, einschließlich externer Dienstleister, mithilfe von Normen empfiehlt:

1. Betreiber kritischer Einrichtungen müssen laut Art. 13 Maßnahmen ergreifen, die erforderlich sind, um „ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten, unter gebührender Berücksichtigung von Maßnahmen wie der Festlegung von Kategorien von Personal, das kritische Funktionen wahrnimmt, der Festlegung von Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen und der Einführung von Verfahren für Zuverlässigkeitsüberprüfungen im Einklang mit Art. 14 und der Benennung von Kategorien von Personal, die solche Zuverlässigkeitsüberprüfungen durchlaufen müssen, und der Festlegung angemessener Schulungsanforderungen und Qualifikationen. (…) Für die Zwecke von Unterabsatz 1 Buchstabe e stellen die Mitgliedstaaten sicher, dass kritische Einrichtungen das Personal externer Dienstleister bei der Festlegung der Kategorien von Personal, das kritische Funktionen wahrnimmt, berücksichtigt“.
2. Laut Art. 16 unterstützen die Mitgliedstaaten Betreiber bei der Erfüllung dieser Maßnahmen durch die Anwendung von europäischen und internationalen Normen.

In die Praxis umgesetzt, wird in beiden Artikeln Betreibern empfohlen, die Qualität beispielsweise von Sicherheitsdienstleistern und deren Personal

auf der Grundlage bestehender Industrienormen wie EN 16082 (Sicherheitsdienste für Flughäfen und die Luftfahrt), EN 16747 (Sicherheitsdienste für die See- und Hafenwirtschaft) und EN 17483 (Sicherheitsdienste für den Schutz kritischer Infrastrukturen) zu kontrollieren.

Diese Empfehlung entspricht einerseits Forderungen des Europäischen Parlaments im bereits erwähnten Bericht 2018/2044 nach spezifischen Qualitätskriterien für die Beschaffung von Sicherheitsdienstleistungen zum Schutz Kritischer Infrastrukturen. Andererseits knüpft die Richtlinie hier an zwei Initiativen der europäischen Sicherheitswirtschaft an:

– Im Zuge der EU-Richtlinie über die öffentliche Auftragsvergabe von 2014 hat die CoESS, gemeinsam mit unserem Sozialpartner UNI Europa und mithilfe von EU-Fördergeldern, einen Leitfaden für Beschaffungsverfahren nach dem „Bestbieter-Prinzip" erarbeitet (verfügbar auf www.secure bestvalue.org).
– Seit Jahren beteiligt sich die CoESS aktiv an der Entwicklung europäischer Normen für das Sicherheitsgewerbe, inklusive EN 16082 (Sicherheitsdienste für Flughäfen und die Luftfahrt), EN 16747 (Sicherheitsdienste für die See- und Hafenwirtschaft) und EN 17483 (Sicherheitsdienste für den Schutz Kritischer Infrastrukturen).

IV. Nächste Schritte: Umsetzung auf nationaler Ebene bis Oktober 2024

Eine EU-Richtlinie ist allerdings nur so gut wie ihre Umsetzung auf nationaler Ebene. Die Mitgliedstaaten müssen bis Oktober 2024 den Vorgaben und Empfehlungen der CER-Richtlinie in nationalen Gesetzgebungsverfahren nachkommen – wobei sie die Möglichkeit haben, strengere Vorschriften einzuführen. Die Empfehlung der CoESS ist es dabei, dass die Politik nun eine Umsetzung des Textes gewährleisten sollte, die der angenommenen Fassung entspricht und die Qualitätskontrollmaßnahmen von Sicherheitsdienstleistern für Betreiber Kritischer Infrastrukturen mit Hilfe existierender Normen effizient und rechtlich bindend durchsetzen.

Die CoESS wird diesen Prozess in Europa begleiten und den Austausch zwischen Mitgliedern fördern. Aktuell (Stand November 2023) haben nur sehr wenige Länder wie Deutschland bereits einen Gesetzesentwurf vorgelegt, der die Vorgaben der CER-Richtlinie umsetzt.