Auswirkungen aktueller Cybersecurity-Richtlinien auf Unternehmen ohne KRITIS-Bezug

The impact of current cybersecurity guidelines on companies without CRITIS relevance

Martin Koop

Die neuen EU-Richtlinien zu Cybersicherheit erweitern die Anforderungen und Anwendungsbereiche für alle Verkehrsunternehmen deutlich, sodass auch aktuelle Nicht-KRITIS-Bahnen verpflichtet sind, gestiegene Cybersicherheitsmaßnahmen umzusetzen. Dies betrifft Eisenbahnverkehrsunternehmen (EVU) und Eisenbahninfrastrukturunternehmen (EIU) gleichermaßen. Die Umsetzung der Richtlinien in deutsche Gesetze ist bereits im Referentenentwurf veröffentlicht, und diese werden in diesem Beitrag vorgestellt.

1 Einleitung

Die fortsetzende Ausgestaltung nationaler und europäischer Cybersecurity-Richtlinien und -Gesetze ist die Antwort auf die steigende Anzahl schwerwiegender Cyberangriffe auf kritische Einrichtungen, besonders im Sektor Transport [1]. In Deutschland definiert dazu bereits seit 2016 das IT-Sicherheitsgesetz (IT-SIG) sowie dessen Ausdetaillierung in der KRITIS-Verordnung (KritisV) einen entsprechenden Maßnahmenkatalog für ausgewählte Kritische Infrastrukturen. In den Geltungsbereich mit KRITIS „Korb II" ab Juni 2017 sind auch die EIU aufgenommen worden.

Auf europäischer Ebene etabliert die Netz- und Informationssicherheits-Richtlinie (NIS-1) einen einheitlichen Cybersicherheitsstandard in der EU, welcher 2016 für den Bereich Verkehr bereits kurzfristig national umgesetzt wurde.

Durch die schwache Wirkung bzw. Divergenz der Umsetzungen in der EU, besonders in gesellschaftlich wichtigen Wirtschaftszweigen, wurde im Dezember 2022 eine überarbeitete NIS-2-Richtlinie veröffentlicht [2]. Die Umsetzung in allen EU-Mitgliedsstaaten muss bis 17. Oktober 2024 in nationales Recht vollzogen werden. Eine Besonderheit in der Richtlinie ist dabei die Ausweitung des Geltungsrahmens, der nun auch mittelgroße Unternehmen ab 50 Mitarbeiter oder 10 Mio. EUR Jahresumsatz einbezieht.

Mit erweiterten Maßnahmenforderungen, erhöhtem Geltungsbereich und einer engeren EU-weiten Koordination soll im Bereich Cybersicherheit der öffentlichen sowie privaten Sektoren eine Verbesserung der Reaktionsfähigkeit entstehen und das Cybersicherheitsniveau in der Europäischen Union erhöht werden.

Zusätzlich zu den regulatorischen Ansätzen der NIS-2-Richtlinie hat die EU mit der Critical Entities Resilience-Richtlinie (CER oder im englischsprachigen Raum meist EU-RCE) den Betrachtungsraum für kritische Sektoren erweitert und fordert unter anderem die physische Resilienz von kritischen Einrichtungen [3].

Entsprechende Anpassungen am IT-Sicherheitsgesetz sowie der KRITIS-Verordnung sind bereits im Entwurf veröffentlicht worden und sollen bis Frühjahr 2024 veröffentlicht werden [4]. Ein wesent-

The new EU directives on cybersecurity have significantly expanded the requirements and areas of application for all transport organisations, so that current non-CRITIS railways are also obliged to implement increased cybersecurity measures. This affects railway undertakings (RU) and railway infrastructure organisations alike. The implementation of the directives into German law has already been published in a draft bill and is presented in this article.

1 Introduction

The continued development of national and European cybersecurity guidelines and laws is the answer to the increasing number of serious cyber-attacks on critical facilities, especially in the transport sector [1]. In Germany, the IT Security Act (IT-SIG) and its elaboration in the CRITIS ordinance (CRITISV) have defined a corresponding catalogue of measures for selected critical infrastructures since 2016. Railway infrastructure organisations were also included within the scope of the CRITIS "Korb II" as of June 2017.

At the European level, the Network and Information Security directive (NIS-1) has established a uniform cybersecurity standard in the EU that had already been implemented nationally for the transport sector in 2016.

The weak impact or divergence of the implementation within the EU, especially in socially important economic sectors, led to a revised NIS-2 directive being published in December 2022 [2]. This must be incorporated into the national law of all EU member states by 17 October 2024. A special feature of the directive involves the extension of the scope to now also include medium-sized companies with 50 or more employees or an annual turnover of EUR 10 million.

The aim of the extended requirements for cybersecurity measures, increased scope and closer EU-wide coordination is to improve the responsiveness of both the public and private sectors in the area of cybersecurity and to raise the level of cybersecurity in the European Union.

In addition to the regulatory approaches of the NIS-2 directive, the EU has also expanded the area of consideration for critical sectors with its Critical Entities Resilience Directive (CER or EU-RCE in English-speaking countries) and requires, amongst other things, physical resilience in critical facilities [3].

The corresponding adjustments to the IT Security Act and the CRITIS regulation have already been published in draft form and should be published by spring 2024 [4]. The increasing incidents related to the manipulation of critical services are the

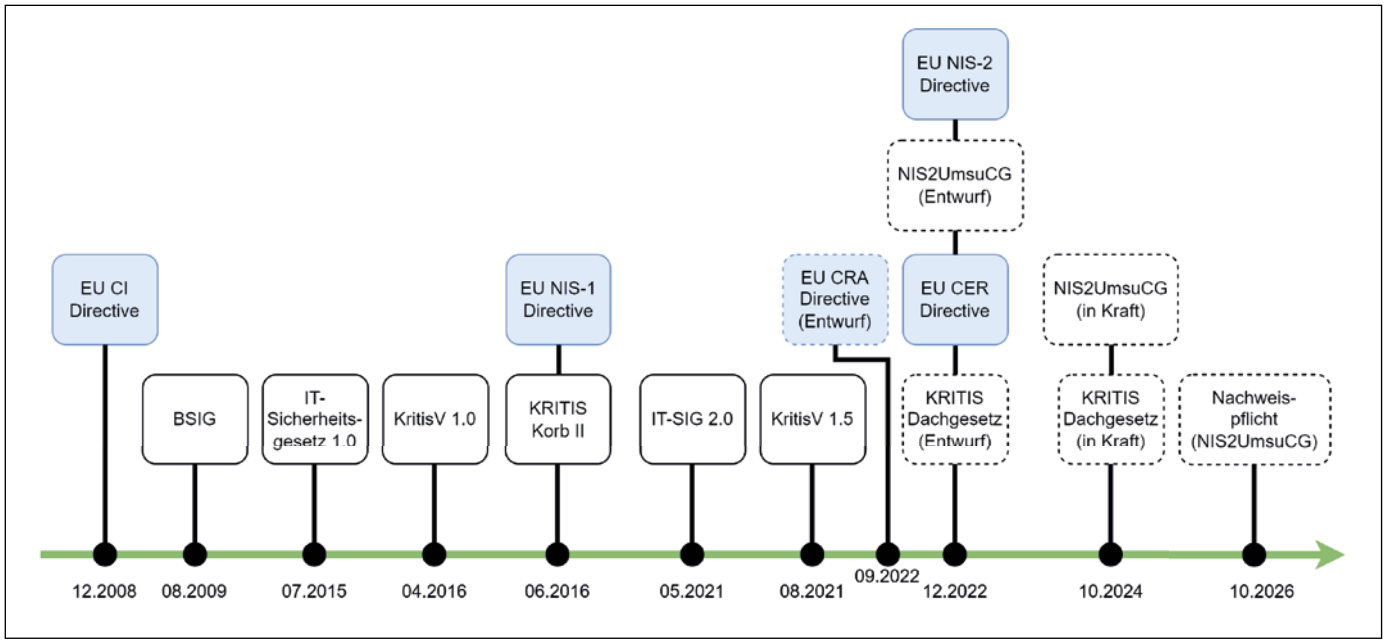

Bild 1: Zeitliche Einordnung veröffentlichter Cybersecurity-Gesetze und -Richtlinien
Fig. 1: The chronological order of the published cybersecurity laws and guidelines
Quelle / *Source*: eigene Darstellung

licher Treiber dieser Maßnahmen sind die zunehmenden Ereignisse im Zusammenhang mit Manipulation von kritischen Dienstleistungen. Zusätzlich steigert der Angriffskrieg der Russischen Föderation auf die Ukraine und damit einhergehende Konflikte die Bedrohungslage. Digitale sowie physische Angriffe auf Kritische Infrastrukturen sind ein immer häufiger zum Einsatz kommendes Druck- und Maßnahmenmittel für kriminelle und kriegerische Handlungen.
Dieser Beitrag soll eine Übersicht der unterschiedlichen Gesetze und Richtlinien aufzeigen (visualisiert in Bild 1), die geforderten Maßnahmen transparent wiedergeben sowie die betroffenen Organisationen benennen.

2 Übersicht wichtiger Cybersecurity-Gesetze und -Richtlinien

2.1 Netz- und Informationssicherheits-Richtlinie (NIS)

Die NIS ist der europäische Rahmen für Mindeststandards in Cybersicherheit und dient dazu, das Cybersicherheitsniveau in der EU zu steigern sowie noch weiter zu vereinheitlichen. Mit den Richtlinien werden einheitliche Sicherheitsmaßnahmen sowie die gleichen Sanktionsmöglichkeiten in allen EU-Mitgliedsstaaten gesetzt.
Mit der Aktualisierung innerhalb NIS-2 steigen einerseits die Cybersecurity-Anforderungen, anderseits werden diese auf eine größere Anzahl (kleinerer) Betreiber kritischer sowie digitaler Dienste ausgeweitet (siehe Abschnitt 4.2). Das liegt maßgeblich daran, dass zukünftig Unternehmen / Organisationen ab 50 Mitarbeiter und 10 Mio. EUR Jahresumsatz betroffen sein werden. Basierend auf Schätzungen des Statistischen Bundesamts wird die Umsetzung in Deutschland etwa 29 000 Unternehmen betreffen. Das ist eine Verfünffachung [5] der Anzahl betroffener Unternehmen. Zu den neuen Anforderungen zählen dabei im Wesentlichen die nachfolgenden Punkte:

- Einführung eines Risikomanagements
- Berichtspflicht bei Sicherheitsvorfällen
- Sicherheit in der Lieferkette
- Business Continuity Management
- Penetrationstests.

major driver for these measures. In addition, the Russian Federation's war on Ukraine and associated conflicts are also increasing the threat level. Both digital and physical attacks on critical infrastructure are becoming an increasingly common method of applying pressure and a means for criminal and belligerent acts.
The purpose of this article is to provide an overview of the different laws and guidelines (depicted in fig. 1) so as to transparently reflect the required measures and name the involved organisations.

2 An overview of the important cybersecurity laws and guidelines

2.1 The Network and Information Security Directive (NIS)

The NIS is the European framework for designating minimum cybersecurity standards and it serves to both increase the level of cybersecurity in the EU and further standardise it. The guidelines stipulate uniform security measures and the same sanction options in all the EU member states.
The update contained in NIS-2 has increased the cybersecurity requirements and extended them to a larger number of (smaller) operators of both critical and digital services (see section 4.2). This is mainly due to the fact that companies / organisations with 50 or more employees and an annual turnover of EUR 10 million will be affected in the future. The Federal Statistical Office has estimated that the implementation will affect about 29,000 companies in Germany. This is a fivefold increase [5] in the number of affected companies. The new requirements essentially include the following points:

- the introduction of risk management
- a reporting obligation for security incidents
- security in the supply chain
- Business Continuity Management (BCM)
- penetration testing

All the new measures are aimed at prevention and should lead to a reduction in the consequences of any security incidents on

Alle neuen Maßnahmen zielen auf vorbeugende Maßnahmen und solche zur Reduzierung der Folgen von Sicherheitsvorfällen auf Nutzer und Umwelt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) forderte bereits ab Mai 2023 mit der „Orientierungshilfe Systeme zur Angriffserkennung (OH SzA)" [6] verbindliche Vorgaben für KRITIS-Betreiber.

Dazu gehört der Aufbau von Security Operation Centers (SOC) bzw. Cybersecurity Incident Response Teams (CSIRT), welche mit Einsatz von Security Information and Event Management (SIEM) Systems die Erkennung und Alarmierung von Security relevanten Ereignissen übernehmen. Voraussetzung ist die Implementierung von Log-Nachrichten aus den Systemen und Netzwerk-Komponenten.

Somit wird der aktive Schutz einerseits vorausgesetzt, andererseits wird damit die Erkenntnis unterstützt, dass Sicherheitsvorfälle nicht sicher ausgeschlossen, ihre Häufigkeit und Auswirkungen nur reduziert werden können. Daher sollte der Fokus auf Vorbereitung und koordinierter Reaktion liegen.

Als Grundlage ist hierfür eine Festlegung zur Analyse von Risiken beim einzelnen Betreiber notwendig (Risikomanagement). Das Risikomanagement der IT-Sicherheit muss sich in das Risikomanagement des Unternehmens integrieren, um insgesamt zu wirken. Die Ergebnisse bilden die Grundlage für wirtschaftliche und wirksame Maßnahmen sowie Identifikation von kritischen Aktivitäten im Zuge eines erfolgreichen Angriffs. Auf Basis der hierbei gewonnenen Erkenntnisse können Konzepte zur Bewältigung von Sicherheitsvorfällen, sowie zum Weiterbetrieb im Falle einer Störung bzw. eines Ausfalls, erstellt werden (Backup, Wiederherstellung, Notfall / Krisenmanagement).

Auf diesen Erkenntnissen basierend, können fundierte Anforderungen an zu liefernde Systeme, deren Entwicklung, Lieferung sowie Inbetriebnahme (IT-Sicherheit der Lieferkette) gestellt werden.

Für den Einkauf bedeutet es die Definition von technischen und organisatorischen Maßnahmen (TOM) für die zu liefernden Produkte und Dienstleistungen. Zusätzlich muss die Einhaltung von Sicherheitsstandards in der Entwicklung, beispielsweise nach IEC 62443, sichergestellt werden.

Außerdem wird der Lieferant in die Verantwortung für das Business Continuity Management durch die kontinuierliche Prüfung auf neue Schwachstellen und Bereitstellung von Software-Updates sowie mitigierende Maßnahmen genommen (Asset- / Patch- / Schwachstellen-Management).

Die Forderung nach Daten- und Transportverschlüsselung sowie Multifaktor-Authentifizierung wird für Betreiber sicherlich eine der schwierigsten Umsetzungsmaßnahmen darstellen. Eine technische Lösungsmöglichkeit kann dabei darin bestehen, den Transport der Daten mit entsprechenden Netzwerk (Krypto)-Komponenten zu schützen, welche beispielsweise mittels Internet Protocol Security (IPsec) die Daten im Netzwerk verschlüsseln. Eine andere (bessere) Realisierung ist, die Daten vom Quell- zum Ziel-System (Ende-zu-Ende) mittels Transport Layer Security (TLS) und dem Einsatz von digitalen Zertifikaten zu verschlüsseln.

Beide Realisierungen setzen allerdings voraus, dass in die Komponenten entsprechende Verschlüsselungsprotokolle und ein unternehmensweites Schlüsselmanagement, z. B. für digitale Zertifikate, meist in Form einer Public-Key-Infrastruktur (PKI), implementiert sind. Die PKI ermöglicht dann die Verschlüsselung der Daten und damit auch einen Integritätsschutz, genauso die Authentifizierung von Systemen untereinander.

Als Qualitätskontrolle werden Penetrationstests verbindlich gefordert. Penetrationstests gehen über funktionale Tests hinaus und simulieren – bis zu einem gewissen Grad – Angriffsversuche,

users and the environment. The German Federal Office for Information Security (BSI) demanded binding requirements for CRITIS operators as early as in May 2023 with the "Orientierungshilfe Systeme zur Angriffserkennung (OH SzA)" [6].

This includes the establishment of Security Operation Centres (SOC) or Cybersecurity Incident Response Teams (CSIRT), which use Security Information and Event Management (SIEM) systems to detect and issue alerts about any security-relevant events. The implementation of log messages from the systems and network components is a prerequisite.

As such, active protection is assumed on the one hand, while the realisation that security incidents cannot be excluded with certainty, but that their frequency and effects can only be reduced is supported on the other hand. Therefore, the focus should be on preparation and a coordinated response.

The determination for the risk analysis at the individual operator's facility is necessary (risk management) as the basis for this. IT security risk management must be integrated into the company's risk management in order to be effective overall. The results form the basis for economic and effective measures as well as the identification of any critical activities over the course of a successful attack. The knowledge gained within this process can be used to create concepts for coping with security incidents, as well as for continued operations in the event of a malfunction or a failure (backup, recovery, emergency / crisis management).

Substantiated requirements can then be set for the systems to be supplied and for their development, delivery and commissioning (IT security in the supply chain) on the basis of these findings.

For purchasing, this means the definition of technical and organisational measures (TOM) for the products and services that are to be delivered. In addition, compliance with the security standards, for example according to IEC 62443, must also be ensured during development.

Furthermore, the supplier is responsible for the business continuity management involving continuous inspections for new vulnerabilities and the provision of software updates, as well as any mitigating measures (asset / patch / vulnerability management).

The requirement for data and transport encryption, as well as multifactor authentication, will certainly be one of the most difficult implementation measures for operators. One technical solution can be to protect the transport of data with appropriate network (crypto) components that encrypt network data using Internet Protocol Security (IPsec). Another (better) implementation involves encrypting the data from the source to the target system (end-to-end) using Transport Layer Security (TLS) and the use of digital certificates.

Both solutions, however, require the components to implement the appropriate encryption protocols and a company-wide key management system, e.g. digital certificates, usually in the form of a Public Key Infrastructure (PKI). The PKI then enables the data encryption and therefore also the integrity protection, as well as the mutual authentication of the systems.

Penetration tests are required as a mandatory type of quality control. Penetration tests go beyond functional tests and simulate – to a certain extent – attempted attacks to prove the successful implementation of any hardening measures, as well as the necessary resilience.

The NIS-2 directive has therefore created a more profound definition of the requirements than the CER directive, which has a broader scope. Tab. 1 shows the scope of requirements according to the current status in comparison with NIS-2, the CER directive and the currently valid CRITIS regulation.

Maßnahmen	NIS 2	CER	KritisV 1.5
Risikobewertung	x	x	x
Wiederherstellungsmanagement (Krisenmanagement)	x	x	x
Vorfallserkennung SOC / CSIRT)	x		x (aktualisiert)
Störfallmeldung	x	x	x
Physische Sicherheit	x	x	x
Lieferketten	x		x
Security Training	x	x	x
ISMS / Richtlinien	x		x
Asset Management	x		x
Security in Einkauf (TOM)	x		
Security in Entwicklung (IEC 62443)	x		
Security in Wartung	x		
(Daten / Transport) Verschlüsselung (PKI)	x		
Schutz bei Zutritt / Zugang / Zugriff	x		
(Multi-Faktor) Authentifizierung (PKI)	x		

Tab. 1: Übersicht der umzusetzenden Maßnahmen

Measures	NIS 2	CER	KritisV 1.5
Risk assessment	x	x	x
Business continuity management (Crisis management)	x	x	x
Security monitoring (SOC / CSIRT)	x		x (updated)
Incident reporting	x	x	x
Physical security	x	x	x
Supply chains	x		x
Security training	x	x	x
ISMS / Policies	x		x
Asset management	x		x
Security in purchasing (TOM)	x		
Security in development (IEC 62443)	x		
Security in maintenance	x		
(Data / Transport) Encryption (PKI)	x		
Identity access management	x		
(Multi-factor) authentication (PKI)	x		

Tab. 1: Overview of the measures to be implemented

um die erfolgreiche Durchführung von Härtungsmaßnahmen sowie die notwendige Resilienz nachzuweisen.

Die NIS-2-Richtlinie schafft somit eine tiefergreifende Anforderungsdefinition als die mit weiterem Betrachtungsraum ausgestattete CER-Richtlinie. Tab. 1 zeigt den Anforderungsumfang nach heutigem Stand im Vergleich zwischen NIS-2, CER-Richtlinie und der aktuell gültigen KRITIS-Verordnung.

2.2 Critical Entities Resilience (CER)

The CER directive is a continuation of the European Critical Infrastructure (EU CI) directive from 2008 [7], which initially only covered the energy and transport sectors. Then, as now, the aim was to strengthen the resilience against threats such as terrorist attacks, sabotage, cyber-attacks and natural hazards. The CER should not be confused with the European Cyber Resilience Act (EU CRA),

2.2 Critical Entities Resilience (CER-Richtlinie)

Die CER-Richtlinie ist die Fortführung der European Critical Infrastructure (EU CI) Richtlinie aus 2008 [7], welche initial nur die Sektoren Energie und Transport umfasste. Damals wie heute wird das Ziel verfolgt, die Widerstandsfähigkeit (Resilienz) gegenüber Bedrohungen wie Terroranschlägen, Sabotage, Cyberangriffen und Naturgefahren zu stärken. Nicht zu verwechseln ist die CER mit dem europäischen Cyber Resilience Act (CRA), welcher ebenso 2022 von der EU als Entwurf veröffentlicht wurde und die Cybersicherheitsanforderungen an den gesamten Lebenszyklus von digitalen Produkten (IT / OT Hardware und Software) darlegt [8].

Äquivalent zur zweiten Version der NIS-Richtlinie werden mit CER weitere kritische Sektoren einbezogen. Mit der Richtlinie verpflichten sich die EU-Staaten, weiterhin regelmäßige Risikobewertungen durchzuführen, um KRITIS-Einrichtungen zu ermitteln und bei der Verbesserung der Resilienz zu unterstützen, beispielsweise durch Leitfäden, Beratung oder Schulung. Die korrekte Umsetzung der Maßnahmen kann durch nationale Stellen kontrolliert und bei Nichterfüllung mit Sanktionen belegt werden.

Betroffene Unternehmen sind hierbei nicht nur zur Prävention von Sicherheitsvorfällen, sondern zusätzlich zur Krisen- sowie Katastrophenvorsorge (inklusive alternativer Lieferketten) verpflichtet. Hierzu zählen besonders die Aspekte der physischen Sicherheit wie Perimeterüberwachung und Zutrittskontrolle. Weiterhin gehört die Gewährleistung eines Business Continuity Managements und die Schulung von Personal (Security Training) zu den neuen gesetzlichen Pflichten.

3 Umsetzung in deutsche Gesetze

Durch die Veröffentlichung der Richtlinie (EU) 2022/255 NIS-2 muss Deutschland bis 17. Oktober 2024 die Umsetzung in ein nationales Gesetz vollziehen. Die Forderungen aus NIS-2 werden im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt [4]. Der Referentenentwurf NIS2UmsuCG ist dabei die Vorlage und ein Artikelgesetz, das die verschiedenen Gesetze anpasst, die Bezug zum Inhalt der NIS-2-Richtline haben.

3.1 Auswirkungen auf das IT-Sicherheitsgesetz (BSIG)

Das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" (BSIG) wird oft als IT-Sicherheitsgesetz (IT-SiG) bezeichnet. Es ist das zentrale Gesetz, welches die Informationssicherheit in Deutschland seit 2015 regelt. Das Gesetz verpflichtet Kritische Infrastrukturen zur Einhaltung angemessener Sicherheitsvorkehrungen und macht das BSI zur zentralen Meldestelle sowie Kontrollinstanz.

Die BSI-Kritis-Verordnung [9] von 2016 ergänzt das Gesetz und regelt konkrete Schwellenwerte für Betreiber kritischer Anlagen. Mit der Aktualisierung im Jahr 2021 wird das Gesetzt oft als IT-Sicherheitsgesetz 2.0 bezeichnet. Die Änderungen waren unter anderem erhöhte Befugnisse des BSI, höhere Strafen, neue KRITIS-Sektoren und Anpassung der Schwellenwerte. Mit dem umfassenden NIS-2-Richtlinienkatalog werden nun die Mindestanforderungen für Cybersecurity übernommen.

Die Schwerpunkte sind hierbei:

- Erweiterung Anzahl der KRITIS-Betreiber
- Definition der Mindestsicherheitsanforderung
- Überarbeitung der Bußgelder
- Zentrale Koordination und Informationsaustausch
- Dreistufige Meldepflicht

1. Jeder erhebliche Sicherheitsvorfall muss unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnisnahme, dem (nationalen) CSIRT gemeldet werden.

which was also published as a draft by the EU in 2022 and sets out the cybersecurity requirements for the entire life cycle of any digital products (IT / OT hardware and software) [8].

Equivalent to the second version of the NIS directive, the CER also includes additional critical sectors. Under the directive, the EU states have continued to commit to conducting regular risk assessments aimed at identifying CRITIS facilities and supporting improvements in resilience, for example by means of guidance documents, advice or training. The correct implementation of the measures can be monitored by national institutions and sanctions can be imposed for non-compliance.

The companies concerned are not only obliged to prevent any security incidents, but also to prepare for crises and disasters (including alternative supply chains). This particularly includes aspects of physical security such as perimeter surveillance and access control. Furthermore, the new legal obligations also include guaranteed business continuity management and personnel training (security awareness).

3 Incorporation into German law

The publication of Directive (EU) 2022/255 NIS-2 means that Germany must incorporate it into its national law by 17 October 2024. The NIS-2 requirements have been implemented in the NIS-2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) [4]. The draft NIS2UmsuCG bill is the template and an omnibus law that amends various laws related to the contents of the NIS-2 directive.

3.1 The effects on the IT Security Act (BSIG)

The "Act on the Federal Office for Information Security" (BSIG) is often referred to as the IT Security Act (IT-SiG). It is the central law that has regulated information security in Germany since 2015. The law obliges critical infrastructures to comply with appropriate security precautions and makes the BSI the central reporting office as well as the control authority.

The BSI-CRITIS ordinance [9] of 2016 supplements the law and regulates concrete threshold values for the operators of critical systems. After the update in 2021, the law is now often referred to as the IT Security Act 2.0. The changes include increased powers for the BSI, higher penalties, new CRITIS sectors and adjusted thresholds. The minimum cybersecurity requirements have now been adopted with the comprehensive NIS-2 policy catalogue.

The focal points here are:

- an increased number of CRITIS operators
- the definition of the minimum safety requirement
- the revision of fines
- the central coordination and exchange of information
- the three-stage reporting obligation

1. Any significant security incident must be reported to the (national) CSIRT immediately or at the latest within 24 hours of becoming aware of it.
2. Incident changes must be reported immediately, at the latest within 72 hours, along with an assessment of the status (severity and impact).
3. Interim reports on relevant changes must be submitted upon request and documented in a detailed final report within one month of notification.

3.2 The new CRITIS Regulation (Umbrella Act)

The CRITIS Regulation (BSI-CRITISV) basically concretises the IT Security Act and defines the threshold values and facilities of

2. Vorfalls-Änderungen müssen unverzüglich, längstens innerhalb von 72 Stunden, zusammen mit einer Bewertung des Status (Schweregrad und Auswirkungen) nachgemeldet werden.
3. Auf Nachfrage müssen Zwischenberichte über relevante Änderungen abgegeben werden und innerhalb eines Monats nach Meldung in einem ausführlichen Abschlussbericht dokumentiert werden.

3.2 Neue KRITIS-Verordnung (Dachgesetz)

Die KRITIS-Verordnung (BSI-KritisV) konkretisiert grundsätzlich das IT-Sicherheitsgesetz und definiert Schwellenwerte und Anlagen betroffener Betreiber. Nach der Veröffentlichung des IT-Sicherheitsgesetzes 2.0 hat die Weiterentwicklung von Cybersecurity-Anforderungen nicht lange auf sich warten lassen. So wurde die KRITIS-Verordnung im Januar 2021 sowie März 2023 aktualisiert, und es wurden neue KRITIS-Anlagen hinzugefügt sowie Anpassungen der Schwellenwerte von Anlagen definiert.

Hervorzuheben sind die Konkretisierungen aus KritisV 1.5, welche die Definitionen von Anlagen und ihrer IT in § 1 definiert:

- IT: Anlagen umfassen bzw. beinhalten neben Betriebsstätten, Einrichtungen und Geräten explizit die Software und IT-Dienste, die für *„die Erbringung notwendig sind"*.
- Anlagen: Mehrere Anlagen in einem betriebstechnischen Zusammenhang für dieselbe kritische Dienstleistung gelten als eine Anlage.
- Betreiber: Werden Anlagen von mehreren Betreibern betrieben, sind alle für die Erfüllung der KRITIS-Pflichten gleichermaßen verantwortlich.

Die EU-Regulierung zu Kritischen Infrastrukturen legt mit NIS-2 und EU CER breitere Sektor-Definitionen fest. Durch die NIS-2-Richtlinie arbeitet das Innenministerium seit 2022 an einem KRITIS-Dachgesetz [10], welches die Anforderungen zu Resilienz und Cybersicherheit an Kritischen Infrastrukturen konkretisieren und die Stärkung der physischen Sicherheit vorgeben soll. Der Schutz Kritischer Infrastrukturen soll damit per Bundesgesetz geregelt werden.

Wesentliche Anpassungen sind dabei:

- Gesetzliche Regelungen zu physischem Schutz und Abhängigkeiten der Sektoren bei Störungen
- Regelung zum Einsatz von kritischen (IT) Komponenten oder Prozessen, um Einflüsse und Abhängigkeiten von nicht nachgewiesen vertrauenswürdigen Herstellern zu verhindern

Anlagen / Systeme	Schwellenwert
Personenbahnhof (§ 4 Abs. 1 und 2 EBO)	höchste Bahnhofskategorie (gebildet nach Stationspreissystem: z. B. >15 Bahnsteigkanten / >280 m Bahnsteiglänge / > 50 000 Reisende am Tag / >1000 Zughalte am Tag
Güterbahnhof (§ 4 Abs. 1 und 2 EBO)	23 000 ausgehende Züge
Zugbildungsbahnhof	23 000 gebildete Züge
Schienennetz und Stellwerke (gemäß § 4 Abs. 3 bis 7 und 10 bis 11 EBO)	deutsches TEN-V Kernnetz (EU) 1315/2013
Verkehrssteuerungs- und Leitsystem (Disposition, Zugbetrieb EIU)	deutsches TEN-V Kernnetz (EU) 1315/2013
Leitzentrale (Überwachung EVU, Instandhaltung Fahrzeuge)	8,2 Mio. Zug-, 730 Mio. Tonnenkilometer (Disponierte Transportleistung: Personen / Güter)
ÖPNV Schienennetz / Leitzentralen im ÖSPV (§ 4 Abs. 1-3 PBefG)	125 Mio. unternehmensbezogene Fahrgäste pro Jahr

Tab. 2: KRITIS-Schwellenwerte im Bereich Eisenbahn

the affected operators. The further development of the cybersecurity requirements was not long in coming after the publication of the IT Security Act 2.0. The CRITIS Regulation was updated in January 2021 and March 2023 and new CRITIS facilities were added and adjustments to the threshold values of facilities were defined.

The concretisations from CRITISV 1.5, which define the definitions for installations and their IT in section 1, should be emphasised:

- IT: In addition to the premises, facilities and equipment, facilities also include the software and IT services that are "*necessary for the performance*".
- Installations: Several installations for the same critical service within a single operating context are considered to constitute one installation.
- Operators: If systems are operated by several operators, all are equally responsible for fulfilling the CRITIS obligations.

The EU regulation on critical infrastructure has set broader sector definitions with NIS-2 and EU CER. The Ministry of the Interior has been working on a CRITIS umbrella law [10], which should specify the resilience and cybersecurity requirements at critical infrastructures and specify the strengthening of physical security based on the NIS-2 directive, since 2022. The protection of critical infrastructures will therefore be regulated by federal law.

Significant adjustments have been included in the process:

- legal regulations on physical protection and dependencies of the sectors in the event of disruptions
- a regulation on the use of critical (IT) components or processes in order to prevent any influences and dependencies on manufacturers that have not been proven to be trustworthy.
- cross-sectoral cooperation
- central malfunction reporting
- the identified physical security requirements for all the critical infrastructure operators in all sectors
- risk management, resilience plans and the general implementation of measures (technical, personnel, organisational).

3.3 Penalties

Under NIS-2, management bodies in particular (boards of directors, management, etc.) will be responsible for monitoring

Plants / Systems	Threshold value
Passenger station (Section 4 (1) and (2) EBO)	Highest station category (Formed according to the station price system: e.g. >15 platform edges / >280 m platform length / > 50,000 passengers per day / >1000 train stops per day
Freight station (Section 4 (1) and (2) EBO)	23,000 outgoing trains
Train formation station	23,000 trains formed
Railway network and signal boxes (according to section 4, subsections 3 to 7 and 10 to 11 EBO)	German TEN-T core network (EU) 1315/2013
Traffic control and guidance system (dispatching, train operation EIU)	German TEN-T core network (EU) 1315/2013
Control centre (RU supervision, vehicle maintenance)	8.2 million train-kilometres, 730 million tonne-kilometres (scheduled transport performance: passengers / goods)
ÖPNV rail network / control centres in ÖSPV (section 4, subsections 1-3 PBefG)	125 million company-related passengers per year

Tab. 2: The CRITIS threshold values in the railway sector

Unternehmen	Mitarbeiter		Umsatz		Bilanz	Sektor (nach NIS-2)
Mittel	50-249	und	> 50 Mio. EUR	oder	< 43 Mio. EUR	Wichtig
	≤ 49	und	10 – 50 Mio. EUR	oder	10 – 43 Mio. EUR	
Groß	≥ 250	oder	≥ 50 Mio. EUR	oder	≥ 43 Mio. EUR	Wesentlich oder Wichtig

Tab. 3: Unternehmensschwellenwerte nach Nis2UmsuCG

Company	Employees		Turnover		Balance sheet	Sector (according to NIS-2)
Medium	50-249	and	> EUR 50 million	or	< EUR 43 million	important
	≤ 49	and	EUR 10 – 50 million	or	EUR 10 – 43 million	
Large	≥ 250	or	≥ EUR 50 million euros	or	≥ 43 million euros	essential or important

Tab. 3: The company thresholds according to Nis2UmsuCG

- Sektorübergreifende Zusammenarbeit
- Zentrales Meldewesen von Störungen
- Idente Vorgaben im Bereich physische Sicherheit für alle Betreiber Kritischer Infrastrukturen in allen Sektoren
- Risikomanagement, Resilienzpläne und allgemeine Maßnahmenumsetzung (technisch, personell, organisatorisch).

3.3 Strafen

Mit Umsetzung der NIS-2 sollen besonders Leitungsorgane (Vorstand, Geschäftsführung etc.) für das Überwachen der Maßnahmen verantwortlich gemacht werden und bei Verstoß auch privat haftbar sein. Das entspricht im Wesentlichen bereits geltendem Recht. Neu ist jedoch, dass ebenso Bußgeldforderungen vom Schadensbegriff umfasst sein sollen.
Die Obergrenze für Bußgelder für kritische Betreiber liegt bei 10 Mio. EUR bzw. 2 % des globalen Jahresumsatzes des Unternehmens. Bei wichtigen Einrichtungen liegt die Obergrenze bei 7 Mio. EUR bzw. 1,4 % des globalen Umsatzes.

4 Wer ist von NIS-2 / CER / KRITIS-Dachgesetz betroffen?

Die NIS-2-Richtline unterteilt die Unternehmen und Organisation in elf wesentliche und sieben wichtige Sektoren. Der Bereich Transport, welcher den Schienenverkehr einschließt, wird einvernehmlich von allen Verordnungen genannt. Durch die neuen Grenzwerte der NIS-2 wird der Geltungsraum noch erweitert. Die konkrete Ausgestaltung, d.h. Formulierung von Einschränkungen auf Basis durchgeführter Risikoanalysen, obliegt dem jeweiligen Staat. Die Schwellenwerte variieren zwischen den Entwürfen der NIS-2 und dem KRITIS-Dachgesetz heute noch.
Im Grundsatz soll das NIS2UmsuCG im März 2024 verkündet werden und am 1. Oktober 2024 in Kraft treten. Die Nachweispflicht zur Umsetzung der Risikoschutzmaßnahmen soll dann zwei bzw. drei Jahre später, d.h. im Oktober 2026 oder 2027, greifen.

4.1 KRITIS-Schwellenwert (aktuell)

Aktuell regulieren noch die Schwellenwerte aus der KRITIS-Verordnung, welche Anlagen zur Kritischen Infrastruktur zählen. Für den Eisenbahnbereich sind diese in Tab. 2 aufgeführt und werden zusätzlich durch die Eisenbahn-Bau- und Betriebsordnung (EBO) [11] definiert.

4.2 NIS-2-Schwellenwerte (neu)

Ob ein Unternehmen die NIS-2-Richtline umsetzen muss, wird nach einer neuen sogenannten „size-cap"-Regel festgestellt. Dabei werden mittlere und große Unternehmen dieser 18 (11+7) Sektoren nach Mitarbeitergröße sowie Umsatz bzw. Bilanz gemäß der Definition von Kleinstunternehmen sowie kleinen und mittleren Unternehmen (KMU) [12] reguliert. Innerhalb der deutschen NIS-2-Umsetzung (Nis2UmsuCG) werden die KMU-Schwellenwerte wie in Tab. 3 aufgeführt noch einmal verschärft:

the measures and will also be privately liable in the event of a breach. This essentially corresponds to the law already in force. What is new, however, is that claims for fines are also to be included in the definition of damage.
The upper limit for any fines for critical operators is EUR 10 million or 2 % of the company's global annual turnover. In the case of critical facilities, the cap is EUR 7 million or 1.4 % of global turnover.

4 Who is affected by the NIS-2 / CER / CRITIS umbrella law?

The NIS-2 guideline divides companies and organisations into eleven essential and seven important sectors. The transport sector, which includes rail transport, is unanimously mentioned in all the regulations. The new NIS-2 limit values have extended the scope even further. The concrete design, i.e. the formulation of any restrictions based on the performed risk analyses is the responsibility of the given state. The threshold values still vary between the drafts of the NIS-2 and the CRITIS umbrella law.
In principle, the NIS2UmsuCG should be promulgated in March 2024 and enter into force on 1 October 2024. The obligation to provide evidence of the implementation of the risk protection measures will then come into effect two or three years later, i.e. in October 2026 or 2027.

4.1 The CRITIS threshold (current)

At present, the threshold values from the CRITIS ordinance still regulate which facilities count as critical infrastructure. These are listed in tab. 2 for the railway sector and have been additionally defined by the Railway Construction and Operation Regulations (EBO) [11].

4.2 NIS-2 thresholds (new)

The requirement for a company to implement the NIS-2 directive is determined according to a so-called new "size-cap" rule. Medium-sized and large companies in these 18 (11+7) sectors are regulated according to employee size and turnover or their balance sheets based on the definition of micro, small and medium-sized enterprises (SMEs) [12]. Within the German implementation of NIS-2 (Nis2UmsuCG), the SME thresholds have been defined as in tab. 3 and are further intensified as listed.
Any special cases are assessed separately. These include companies with a market monopoly or those that operate across borders. Likewise, all the operators of critical facilities are affected by the required measures, regardless of their size.

5 A summary of the consequences for the railway sector

5.1 Who must implement measures

The new IT Security Act (or NIS2UmsuCG) and the so-called CRITIS umbrella law are currently only available in drafts. The

Sonderfälle werden separat bewertet. Dazu zählen Unternehmen mit Marktmonopol oder solche, die grenzüberschreitend operieren. Genauso sind alle Betreiber kritischer Anlagen unabhängig von ihrer Größe von den geforderten Maßnahmen betroffen.

5 Die Konsequenzen im Sektor Eisenbahn in der Zusammenfassung

5.1 Wer muss Maßnahmen umsetzen

Das neue IT-Sicherheitsgesetz (bzw. NIS2UmsuCG) und das sogenannte KRITIS-Dachgesetz liegen erst in Entwürfen vor. Basierend auf den Entwürfen und den zugrundeliegenden Richtlinien aus NIS-2 sowie EU CER sind die folgenden Anforderungen sicher:
Alle bisherigen KRITIS-Betreiber bleiben KRITIS-Betreiber. KRITIS-Betreiber werden ohne Einschränkung die erweiterten Anforderungen der europäischen Gesetzgebung, angewendet auf deutsches Recht, umsetzen müssen. Das sind heute alle großen Infrastrukturbetreiber sowie die meisten Betreiber des Öffentlichen Personennahverkehrs (ÖPNV) in den 15 sogenannten großen Großstädten.
Neu hinzu kommen mittlere Unternehmen, d. h. Unternehmen mit mehr als 49 Mitarbeitern oder ab 10 Mio. EUR Jahresbilanz. Welche Einschränkungen die deutsche Gesetzgebung in der Konkretisierung treffen wird, ist noch nicht abzusehen. Werden keine Einschränkungen getroffen, weitet sich der Geltungsbereich auf viele der ÖPNV-Betreiber der kleinen Großstädte (über 100 000 Einwohner) aus. Zusätzlich wird eine Vielzahl reiner EVU hinzukommen. Die-

following requirements are certain based on the drafts and the underlying guidelines from both NIS-2 and EU CER:
All the existing CRITIS operators will remain CRITIS operators. CRITIS operators will have to implement the extended European legislation requirements applied to German law without any limits. This currently means all the major infrastructure operators, as well as most operators of local public transport in the 15 so-called major cities.
Medium-sized companies, i.e. companies with more than 49 employees or an annual balance sheet of EUR 10 million or more, have been newly added to the list. It is not yet clear what restrictions the German legislation will impose. If no restrictions are imposed, the scope of application will expand to include many of the public transport operators in small cities (over 100,000 inhabitants). In addition, many RU will also be added. These are currently only indirectly affected, but will be directly affected in the future.
In addition to infrastructure managers and railways, medium and large service companies could also be covered by the CRITIS provisions, especially if they are involved in activities related to the production, operation or maintenance of transport services.

5.2 Who has to implement what?

There is no differentiation of implementation between company sizes or types. This means that the newly added companies will have to implement the same measures as the current

se sind heute nur indirekt betroffen und würden neu direkt betroffen sein.
Zusätzlich zu den Betreibern der Infrastruktur und Eisenbahnen könnten mittelgroße und große Dienstleistungsunternehmen unter die KRITIS-Bestimmungen fallen, insbesondere wenn sie an Tätigkeiten zur Herstellung, dem Betrieb oder der Aufrechterhaltung der Verkehrsdienstleistung beteiligt sind.

5.2 Wer muss was umsetzen?

Es ist keine Differenzierung der Umsetzungsstärke zwischen der Unternehmensgröße oder -art vorgesehen. D. h., die neu hinzukommenden Unternehmen werden die gleichen Maßnahmen wie heutige KRITIS-Unternehmen umsetzen müssen. Die Liste der geplanten Maßnahmen im aktuellen Entwurf ist in Abschnitt 3.2 aufgeführt.
Für alle Unternehmen sind nach heutigem Stand gleiche Fristen zur Umsetzung der Maßnahmen vorgesehen. D. h., unabhängig vom Ist-Stand müssen bis voraussichtlich Oktober 2026, spätestens Oktober 2027 die Maßnahmen umgesetzt sein.
Aus den praktischen Erfahrungen der KRITIS-Gesetzgebung heißt „umgesetzt" nicht automatisch, dass alle Maßnahmen abgeschlossen sind. Allen beteiligten Parteien im Sektor ist bewusst, dass die sofortige Umsetzung von Maßnahmen mit Auswirkung auf Bestandstechnik Kompromisse erfordert. Trotzdem müssen schlüssige Planungen für Bestands- und Neubausysteme vorliegen, und die Umsetzung muss erkennbar sein. Es ist zu erwarten, dass die Anforderungen an die Umsetzungsgeschwindigkeit und -qualität steigen, da sich der gesamte Verkehrssektor bereits seit 2017 auf diese Situation einstellen konnte. Im Oktober 2027 werden also bereits zehn Jahre seit der Initialisierung von KRITIS im Verkehrssektor vergangen sein.

5.3 Was jetzt zu tun ist

Heutige KRITIS-Betreiber haben bereits die Grundlagen für das Management von IT-Security eingeführt. Das sind im Wesentlichen:
1. Definition des Geltungsbereichs oder „System under Consideration"
2. Die Einführung eines Informations-Sicherheitsmanagementsystems (ISMS), meist auf Basis ISO 27001
3. Die Einführung oder Verbesserung des Assetmanagements zur Erfassung relevanter Informationen für die IT-Sicherheit (z. B. Software-Patches bei Schwachstellen)
4. Die Durchführung einer initialen Risikobewertung (IEC 62443) oder Schutzbedarfsfeststellung (ISO 27001) zur Ermittlung der Kritikalität der einzelnen Assets – basierend auf den zu erwartenden Auswirkungen bei erfolgreicher Manipulation
5. Die Durchführung einer detaillierten Risikoanalyse mit entsprechender Maßnahmenplanung (nach IEC 62443, ISO 27001, IDW-Katalog des BSI)
6. Die Planung und Umsetzung der identifizierten Maßnahmen.

KRITIS-Betreiber können diese Grundlagen nutzen und die durchgeführten Risikoanalysen überarbeiten und die Maßnahmenlisten entsprechend erweitern. Es ist davon auszugehen, dass einige Security-Analysen der KRITIS-Betreiber bereits eine Vielzahl der neu geforderten Maßnahmen in ihrer Maßnahmenplanung haben. Dies ist nicht überraschend, da die europäische und deutsche Gesetzgebung letztendlich nur auf dem Stand der Technik aufsetzt. Dieser Stand der Technik wird für IT-Sicherheit in den Normen ISO 27001 und IEC 62443 international gültig abgebildet. Unternehmen, die neu in den Kreis der KRITIS-Relevanz aufgenommen werden, müssen wahrscheinlich diese Grundlagen noch nachweisen.
Die wesentliche Grundlage bilden:
1. Der Geltungsbereich
2. Ein ISMS mit Assetmanagement.

CRITIS companies. The list of planned measures can be found in section 3.2 of the current draft.
As of today, the same deadlines for implementing the measures are foreseen for all companies. This means that regardless of the current status, the measures will have to be implemented by October 2026 or October 2027 at the latest.
From the practical experience of CRITIS legislation, "implemented" does not automatically mean that all the measures will have been completed. All the parties involved in the sector are aware that the immediate implementation of the measures affecting existing technology requires compromises. Nevertheless, coherent plans for existing and new building systems must be in place and the implementation must be identifiable. It is to be expected that the demands placed on implementation speed and quality will increase, as the entire transport sector has been able to prepare for this situation since 2017. October 2027 will be ten years since the initialisation of CRITIS in the transport sector.

5.3 What has to be done now

Today's CRITIS operators have already introduced the basics for managing IT security. These are essentially:
1. defining the scope or "system under consideration"
2. the introduction of an Information Security Management System (ISMS), mostly based on ISO 27001
3. the introduction or improvement of asset management aimed at acquiring the relevant information for IT security (e.g. software patches in the case of vulnerabilities).
4. conducting an initial risk assessment (IEC 62443) or protection needs assessment (ISO 27001) to determine the critical nature of each asset – based on the expected impact of any successful tampering.
5. the performance of a detailed risk analysis with corresponding action planning (according to IEC 62443, ISO 27001, BSI IDW catalogue)
6. the planning and implementation of the identified measures

CRITIS operators can use this basis to revise the completed risk analyses and expand the lists of measures accordingly. It can be assumed that some CRITIS operators' security analyses already have a large number of newly required measures in their measure planning. This is not surprising, as the European and German legislation is ultimately only based on the state of the art. This state of the art is mapped for IT security in the internationally valid ISO 27001 and IEC 62443 standards. Companies that have been newly included within the circle of CRITIS relevance will probably still have to substantiate these basics.
The essential foundation is formed by:
1. the scope
2. an ISMS with asset management

A comprehensible risk analysis and the planning of the necessary measures are only possible on this basis. The basis is of particular importance given that the risk analyses must be regularly repeated (annually according to the legislation, in practical terms every two years). The quality of the definition and the chosen documentation is decisive for the effort required during each repetition.
Timely IT security requirements for new acquisitions have the great advantage that the number of mitigating measures for existing technology can be drastically reduced. Even though replacement measures initially appear cheap, it is often resource-intensive to maintain them on a permanent basis.

Erst mit dieser Basis sind eine nachvollziehbare Risikoanalyse und Maßnahmenplanung möglich. Da die Risikoanalysen regelmäßig (jährlich nach Gesetzgebung, praktikabel alle zwei Jahre) wiederholt werden müssen, kommt diesen Grundlagen eine besondere Bedeutung zu. Die Qualität der Definition und der gewählten Dokumentation entscheidet maßgeblich über den Aufwand bei der Wiederholung.
Die rechtzeitige Forderung von IT-Sicherheit für Neuanschaffungen hat den großen Vorteil, dass sich die Anzahl mitigierender Maßnahmen für Bestandstechnik drastisch reduzieren lässt. Zwar erscheinen Ersatzmaßnahmen zunächst günstig, jedoch sind sie häufig in der dauerhaften Aufrechterhaltung ressourcenintensiv.

6 Fazit

Die neuen und überarbeiteten EU-Richtlinien NIS-2 und ihre Begleiter müssen in nationales Recht überführt werden. Nach aktueller Planung wird die nationale Gesetzgebung im Oktober 2024 in Kraft treten und zwei, maximal drei Jahre Umsetzungszeit erlauben. Die Umsetzungsfristen gelten europaweit. Heutige KRITIS-Unternehmen können bereits gut vorbereitet sein oder sind bereits in der Umsetzung der neuen Maßnahmen. Für neue Unternehmen im Geltungsbereich der Gesetzgebung ist der notwendige Hub sehr hoch. Es ist zu empfehlen, die Grundlagen für Risikomanagement frühzeitig zu legen, um die erste Auditierung erfolgreich zu bestehen. Die Qualität der Grundlage entscheidet über den Aufwand und den Erfolg der folgenden Jahre im Management der IT-Sicherheits-Maßnahmen, denn IT-Sicherheit ist ein Prozess, kein Zustand. ■

6 Conclusion

The new and revised EU NIS-2 directives and their companions have to be incorporated into national law. According to current planning, the national legislation will come into force in October 2024 and allow two or a maximum of three years for implementation. The implementation deadlines will apply across Europe. Current CRITIS companies may already be well prepared or already in the process of implementing the new measures. The necessary speed is very high for those companies newly included within the scope of the legislation. It is recommended that the risk management foundations should be laid at an early stage in order to successfully pass the first audit. The quality of these foundations determines the effort and success of the following years in the management of IT security measures, because IT security is a process, not a state. ■

LITERATUR | LITERATURE
[1] ENISA: ENISA Threat Landscape: Transport Sektor, 2023
[2] EU 2022/2555: Richtlinie zu Cybersicherheit von Netz- und Informationssystemen, 2022
[3] EU 2022/2557: Richtlinie zur Stärkung der Resilienz kritischer Einrichtungen, 2022
[4] Bundesministerium des Innern und für Heimat (BMI): Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie; https://ag.kritis.info/wp-content/uploads/2023/07/NIS2UmsuCG-Referentenentwurf-BMI-CI1-Bearbeitungsstand-03072023.pdf, 31.07.2023
[5] BMI: EU-Richtlinien zum Schutz Kritischer Infrastrukturen; https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2023/01/eu-richtlinien-kritis.html, 31.07.2023
[6] BSI: Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf, 31.07.2023
[7] EU 2008/114: Richtlinie zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen, 2008
[8] EU 2022/0272: Cybersicherheitsanforderungen für Produkte mit digitalen Elementen; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en, 31.07.2023
[9] Bundesministerium der Justiz (BMJ): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV), 2023
[10] BMI: Eckpunkte für das KRITIS-Dachgesetz; https://dserver.bundestag.de/btd/20/054/2005491.pdf, 31.07.2023
[11] BMJ: Eisenbahn-Bau- und Betriebsordnung; https://www.gesetze-im-internet.de/ebo/BJNR215630967.html, 31.07.2023
[12] EU 2003/361/EC; Kleinstunternehmen sowie kleine und mittlere Unternehmen: Definition und Umfang, 2016

AUTOR | AUTHOR

Dr. Ing. Martin Koop
Senior Expert IT-Security
Incyde GmbH
Anschrift / *Address*: Schaumainkai 91, D-60596 Frankfurt a. M.
E-Mail: martin.koop@incyde.com