Verlagsbeilage, Dezember 2025

Special
NIS-2
Lösungen und Services

‹kes›
Die Zeitschrift für Informations-Sicherheit

Mitherausgeber

DECOIT®
F24
ibi systems
ISACA
TTS

Impressum

DATAKONTEXT GmbH

Augustinusstraße 11 A
50226 Frechen (DE)
Tel.: +49 2234 98949–30,
redaktion@datakontext.com,
www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Handelsregister:
Amtsgericht Köln, HRB 82299

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel.: +49 6728 289003, anzeigen@kes.de

Satz: Dirk Hemke (SatzPro), Krefeld;
Markus Miller (Satz + Bild), München

Druck: QUBUS media GmbH,
Beckstraße 10, 30457 Hannover

Bild: Adobe Stock/ImageKing

NIS-2 umsetzen mit Multi-Compliance-Framework

Mit der Überführung der NIS-2-Richtlinie in deutsches Recht steigen die Anforderungen an Unternehmen, ihre Informationssicherheit strukturiert und nachvollziehbar zu steuern. Anstatt jede gesetzliche Vorgabe isoliert zu betrachten, ermöglicht ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 in Verbindung mit einem Multi-Compliance-Ansatz eine effiziente und transparente Umsetzung mehrerer Regelwerke.

Von Benjamin Weiß, TTS Trusted Technologies and Solutions GmbH

Das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (im Folgenden NIS-2-Gesetz genannt) erweitert den Anwendungsbereich früherer Regelungen erheblich und konfrontiert bereits regulierte Unternehmen mit zusätzlichen Anforderungen.

Auf den ersten Blick beschreibt das NIS-2-Gesetz einen Katalog von Pflichtanforderungen für betroffene wichtige und besonders wichtige Einrichtungen. Die Risikomanagementmaßnahmen in § 30 (2) stellen dabei einen zentralen Aufwandstreiber für die Einrichtungen dar. Die genannten Maßnahmen dürfen aber keineswegs einfach unreflektiert abgearbeitet oder umgesetzt werden. Das Gesetz verlangt vielmehr einen risikobasierten Ansatz, der die Besonderheiten und Risiken jeder betroffenen Einrichtung berücksichtigt.

Das NIS-2-Gesetz gibt für diese Maßnahmen keine detaillierten Umsetzungsanweisungen vor, sondern fordert die Einhaltung des Standes der Technik sowie die Berücksichtigung einschlägiger nationaler und internationaler Normen. Der aktuelle „Stand der Technik“ lässt sich demnach zum Beispiel anhand von Normen und Standards wie DIN oder ISO bestimmen. Als bekannte Referenzen können daher besonders die ISO/IEC 27001 sowie die begleitende ISO/IEC 27002 mit konkreten Umsetzungshinweisen zur Hand genommen werden.

In Anbetracht eines ISMS nach ISO/IEC 27001 zeigt sich bei den betroffenen Einrichtungen eine heterogene Ausgangslage. Einige verfügen bereits über ein (zertifiziertes) ISMS nach ISO/IEC 27001, andere stehen noch am Anfang. Für die Umsetzung des NIS-2-Gesetzes ist es von großem Vorteil, wenn bereits ein ISMS nach ISO/IEC 27001 besteht und damit auch Maßnahmen aus dem An-

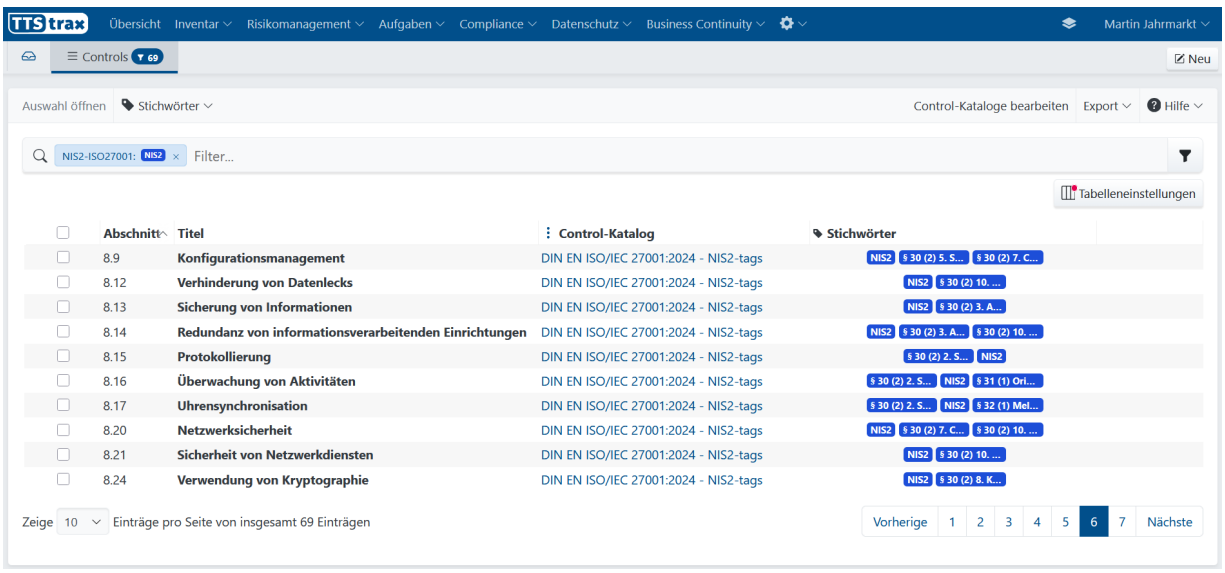


Abbildung 1: Mapping zwischen ISO/IEC 27001-Controls und NIS-2-Anforderungen über Stichwörter-Funktion in TTS trax. (Bild: TTS Trusted Technologies and Solutions GmbH)

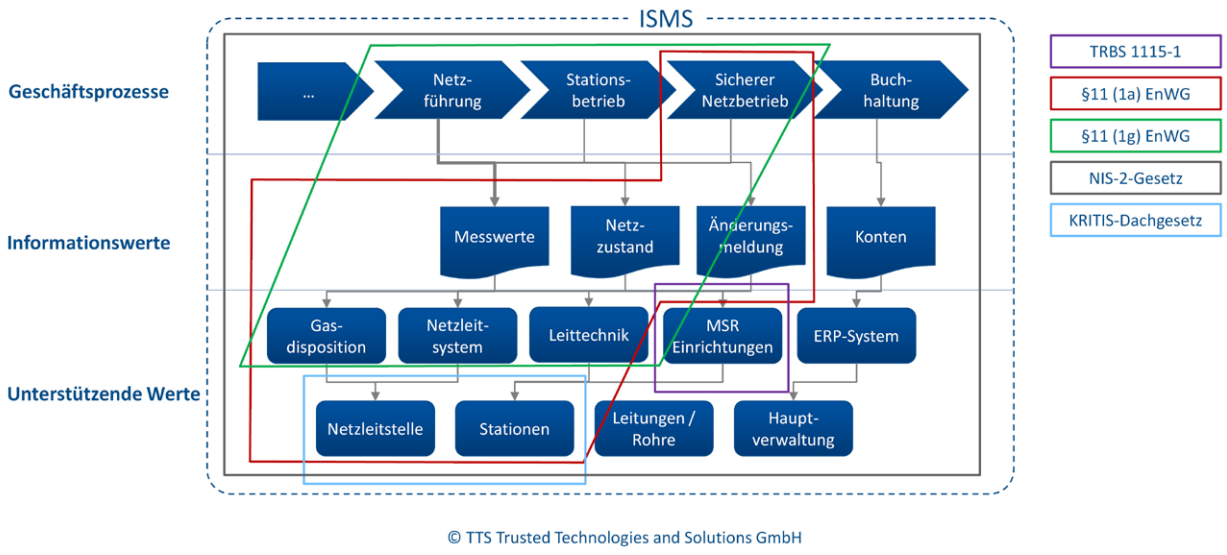


Abbildung 2: Multi-Scope am Beispiel eines Energienetzbetreibers. (Bild: TTS Trusted Technologies and Solutions GmbH)

hang A realisiert sind, da es Überschneidungen mit den Anforderungen aus dem NIS-2-Gesetz gibt. Darüber hinaus ermöglichen die etablierten ISMS-Prozesse eine systematische und nachvollziehbare Umsetzung des NIS-2-Gesetzes.

Mapping zwischen NIS-2-Gesetz und ISO/IEC 27001

Da nicht alle Inhalte des NIS-2-Gesetzes gleichermaßen für jeden Geltungsbereich der verschiedenen Einrichtungen relevant sind, müssen nur die jeweils zutreffenden Anforderungen umgesetzt werden. Nach einer grundsätzlichen Betroffenheitsprüfung sollte zunächst identifiziert werden, welche NIS-2-Anforderungen verpflichtend einzuhalten sind.

Die identifizierten Anforderungen, besonders die aus § 30 des NIS-2-Gesetzes, sind für viele Einrichtungen die größten Aufwandstreiber bei der Umsetzung der gesetzlichen Vorgaben. Diese Anforderungen lassen sich bestehenden Maßnahmen aus dem Anhang A der ISO/IEC 27001 zuordnen. Das Mapping schafft im Rahmen einer GAP-Analyse eine klare und strukturierte Übersicht über den aktuellen Umsetzungsstand. So erkennt eine Einrichtung, in welchen Bereichen sie bereits konform ist und wo noch Handlungsbedarf besteht.

Die Vorgehensweise des Mappings von Anforderungen mit einem ISMS nach ISO/IEC 27001 ist effizient und zielführend. Eine große Zahl der generisch formulierten Anforderungen des § 30 NIS-2-Gesetzes entsprechen den durch die ISO/IEC 27001 implementierten Prozessen und umgesetzten Maßnahmen. Dies kann in einer Einrichtung dazu führen, dass ein Teil, wenn nicht sogar ein Großteil der Anforderungen bereits als umgesetzt angesehen werden kann. Das erläuterte Mapping minimiert demnach den Umsetzungs- und damit auch den Ressourcenaufwand.

Multi-Compliance-ISMS

Die beschriebene Methodik zum NIS-2-Gesetz lässt sich auch auf weitere gesetzliche und regulatorische Rahmenwerke übertragen. Mit diesem Multi-Compliance-Ansatz können mehrere Anforderungskataloge effizient für verschiedene Geltungsbereiche innerhalb einer Einrichtung abgebildet werden.

Durch die jeweils verschiedenen, sich aber teils überlappenden Geltungsbereiche von Gesetzen und Regularien mit häufig sehr ähnlichen Anforderungen innerhalb einer Einrichtung lässt sich der Multi-Compliance-Ansatz mit einem Multi-Scope-Ansatz kombinieren. Ein konkretes Beispiel hierfür ist ein Energienetzbetreiber, der zukünftig folgende Anforderungen berücksichtigen muss:

- Sicherheitskatalog nach § 11 (1a) sowie § 11 (1 g) EnWG (beides künftig § 5c EnWG),
- NIS-2-Gesetz,
- KRITIS-Dachgesetz,
- Gefährdungsbeurteilungen gemäß TRBS 1115–1.

Alle genannten Regelwerke verlangen risikoorientierte Maßnahmenableitung und -umsetzung. Im wirtschaftlichen Interesse eines Unternehmens sollte dies mit einem möglichst geringen Aufwand an Zeit und Ressourcen geschafft werden. An dieser Stelle kommt das bereits erläuterte Mapping zwischen Anforderungen und die damit einhergehende Vorgehensweise zur Umsetzung von Regelwerken zum Einsatz:

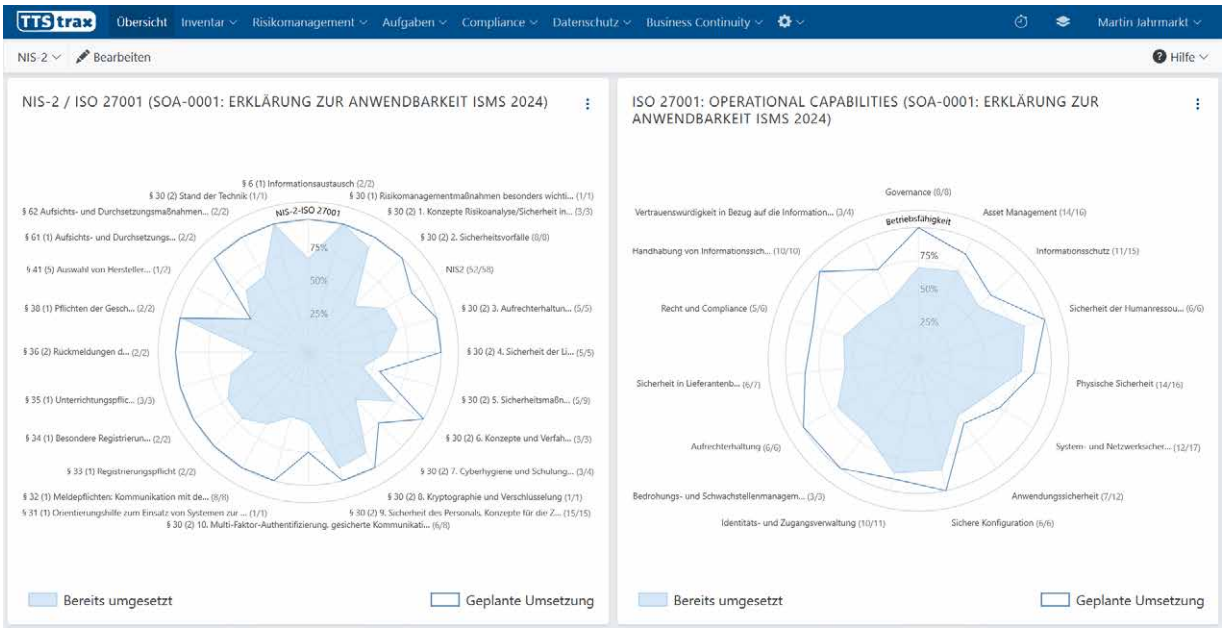


Abbildung 3: Gegenüberstellung von NIS-2-Konformität und ISO/IEC 27001-Umsetzung in TTS trax (Bild: TTS Trusted Technologies and Solutions GmbH)

_____ Auswahl eines Basiskatalogs an Maßnahmen, der den Stand der Technik repräsentiert, zum Beispiel Anhang A der ISO /IEC 27001 oder ein unternehmensspezifisches Regelwerk.
_____ Erstellung eines Mappings für jedes Regelwerk zum Basiskatalog. Da die Maßnahmen des Basiskataloges bereits risikobasiert umgesetzt sind, müssen die Pendants des neuen Regelwerks nicht nochmal, sondern gegebenenfalls nur kleinere Differenzen umgesetzt werden.
_____ Anschließend Umsetzung aller Maßnahmen aus einem Regelwerk, die kein Pendant im Basiskatalog haben.

Damit dieser Ansatz funktioniert, muss es im Unternehmen eine zentrale Stelle geben, welche die Umsetzung solcher gesetzlichen Anforderungen koordiniert. Das kann beispielsweise die Informationssicherheit beziehungsweise der CISO sein. Ist dies der Fall, ergeben sich durch den Multi-Compliance-Ansatz eine Reihe von Vorteilen:

_____ Geringer Zusatzaufwand für die Umsetzung von Anforderungen weiterer Regelwerke, die einem bestehenden Basiskatalog zugeordnet werden können.
_____ Bei Verwendung des Anhang A der ISO/IEC 27001 als Basiskatalog wird dies international anerkannt und kann im Kontext von Marketing und Vertrieb verwendet werden.
_____ Die Konformität zu jedem der Regelwerke kann nach innen, zum Beispiel für die Unternehmensleitung oder nach außen, zum Beispiel im Rahmen von Audits und Prüfungen, dargestellt werden.

Tool-gestützte Effizienz und Transparenz

Für die Erstellung und Nutzung des Mappings zwischen ISO/IEC 27001 inklusive Anhang A und den Maßnahmen aus NIS-2 § 30 ist prinzipiell kein besonderes Tool notwendig. Dies funktioniert grundsätzlich auch mit den Bordmitteln zur Tabellenkalkulation einer jeden Einrichtung.

Spezielle Anwendungen wie das ISMS Tool TTS trax erleichtern jedoch die Arbeit an sich und erhöhen die Effizienz. Über die Nutzung der Stichwörter-Funktion werden (1) heterogene Geltungsbereiche verschiedener Gesetze und Regulatorien erzeugt und (2) Mappings zwischen den verschiedensten Anforderungen eines Multi-Compliance-Frameworks erstellt und dokumentiert.

Es erfolgt eine Homogenisierung der Betrachtungs- und Anforderungslandschaft innerhalb einer Einrichtung. Durch Anwendung der umfassenden Filtermöglichkeiten von TTS trax können Unternehmen ohne großen Aufwand den Umsetzungsgrad verschiedener Anforderungen für jeden beliebigen Geltungsbereich ermitteln und aufzeigen. Eine Prüf- und Nachweisfähigkeit ist hiermit jederzeit gegeben.

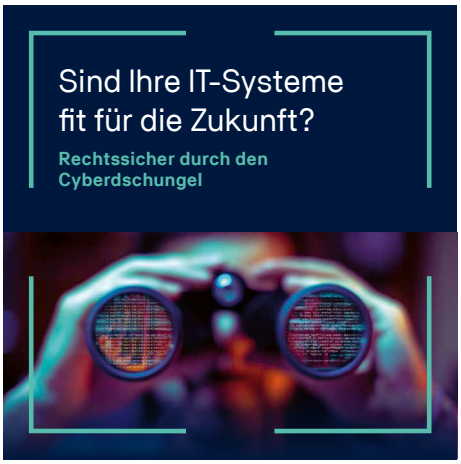
Fazit

Die nachhaltige Umsetzung der NIS-2-Anforderungen gelingt am besten, wenn Einrichtungen ihr ISMS als strategisches Instrument verstehen und gezielt zur Steuerung gesetzlicher Verpflichtungen einsetzen. Durch die Verknüpfung mit einem Multi-Compliance-Ansatz können mehrere gesetzliche und regulatorischen Vorgaben gleichzeitig erfüllt und Synergien genutzt werden. Unterstützt durch ein geeignetes Tool wird dies nicht nur effizienter, sondern auch nachvollziehbar und prüfsicher dokumentiert. ■

TÜVNORD

Cybersicherheit ist Chefsache – Sind Sie bereit für NIS-2?

Die neue EU-Richtlinie NIS-2 (Network and Information Security) verändert alles:



Wer jetzt nicht handelt, riskiert Bußgelder in Millionenhöhe – und persönliche Haftung. Besonders betroffen sind mittelständische Unternehmen aus 18 Sektoren.

Warum gerade jetzt? Die Richtlinie ist eine Antwort auf die digitale Realität:

- Cyberangriffe nehmen zu – allein in Deutschland liegt der jährliche Schaden bei über 200 Milliarden Euro.
- Digitalisierung beschleunigt sich – vernetzte Lieferketten schaffen neue Risiken.
- Resilienz wird zur Pflicht – die EU will ihre digitale Souveränität sichern und systemischen Schocks standhalten.

Was bedeutet NIS-2 für Ihre Organisation?
Die Anforderungen sind klar: Cybersicherheit wird zur Pflichtaufgabe der Geschäftsleitung. Unternehmen ab 50 Mitarbeitenden oder 10 Mio. € Umsatz müssen handeln. Die Richtlinie verlangt verbindliche Standards – vom Risikomanagement über Lieferkettensicherheit bis zur Schulungspflicht.

Stellen Sie sich folgende Fragen:

- Ist Ihre Geschäftsleitung ausreichend geschult in Cybersicherheitsfragen?
- Haben Sie ein dokumentiertes Risikomanagement nach Art. 21 NIS-2?
- Sind Ihre Meldeprozesse bei Sicherheitsvorfällen klar geregelt?

Ihre Vorteile durch gezielte Weiterbildung:

- ✓ Rechtssicherheit durch fundiertes Wissen zu NIS-2 und BSIG-neu
- ✓ Schutz vor Haftungsrisiken durch geschulte Führungskräfte
- ✓ Wettbewerbsvorteil durch nachweisbare Cyberresilienz

Jetzt handeln! Die TÜV NORD Akademie bietet praxisnahe Seminare zur NIS-2-Umsetzung – speziell für Führungskräfte und Verantwortliche aus betroffenen Branchen. Schließen Sie Ihr Wissens-Gap und erweitern Sie Ihre Kompetenzen für die Zukunft, damit Ihre Führungskräfte wissen, was bei einem Cybervorfall zu tun ist und Sie Ihre Pflichten gegenüber dem BSI erfüllen.

Hören Sie unseren Podcast „Wissen kompakt“ Episode:
Cybersicherheit ist Chefsache
NIS-2 im Fokus – Unwissenheit (bei der Cybersicherheit) schützt vor Strafe nicht.

www.tuev-nord.de/podcast-nis2

Lesen Sie unseren vollständigen Blogartikel zur NIS-2 Richtlinie:
www.tuev-nord.de/wissen/nis2

Ein Schutzschild für Ihr Business!
Mit unseren Weiterbildungen qualifizieren Sie sich oder Ihre Mitarbeitenden für diese wichtigen Aufgaben und setzen die hohen Anforderungen der NIS-2-Richtlinie an Unternehmen sicher um.
Stellen Sie die Weichen für eine starke IT-Sicherheit in Ihrem Unternehmen!

Alle Details zu den **TÜV NORD Akademie** Seminaren zur **NIS-2-Richtlinie**

Seminar
Cybersecurity und IT-Strategie für Geschäftsführung und leitende Mitarbeitende
IT strategisch führen, Risiken beherrschen und Pflichten der Geschäftsführung erfüllen

Seminar-Nr.: 10201531 im Shop
www.tuev-nord.de/seminare

Governance, Risk und Compliance aus einer Hand

TopEase bündelt NIS-2-Compliance und digitale Resilienz

Die NIS-2-Richtlinie verlangt von Unternehmen ein höheres Maß an Transparenz, Sicherheit und organisatorischer Verantwortung. Sie verpflichtet dazu, Risiken systematisch zu erkennen, Informationssicherheit nachweisbar zu steuern und die digitale Widerstandsfähigkeit der gesamten Organisation zu stärken. Mit TopEase bietet F24 eine integrierte Plattform, die all diese Anforderungen in einer Lösung vereint.

Von Timo Lutzenberger, F24

Die NIS-2-Richtlinie verändert die Sicherheitslandschaft Europas tiefgreifend. Sie verlangt von Unternehmen und Behörden ein neues Niveau an Transparenz, Verantwortlichkeit und digitaler Resilienz. Besonders betroffen sind Betreiber kritischer Infrastrukturen. Vom Energiesektor über Finanzdienstleister bis hin zur öffentlichen Verwaltung. Doch wie lässt sich dieser neue Ordnungsrahmen in die Praxis überführen, ohne den Überblick zu verlieren?

TopEase, die integrierte Governance-, Risk- und Compliance-Plattform von F24, unterstützt Organisationen dabei Struktur, Transparenz und Nachvollziehbarkeit zu schaffen und ermöglicht so die ganzheitliche Umsetzung der NIS-2-Anforderungen.

NIS-2 fordert ein Umdenken in Governance und Sicherheit

Die neue Richtlinie geht weit über klassische IT-Sicherheit hinaus. Sie verlangt eine organisationsweite Verantwortung für Informationssicherheit, Risikomanagement, Business Continuity und Lieferkettenresilienz. CIOs, CISOs und IT-Leiter stehen damit vor der Aufgabe, technische, organisatorische und regulatorische Maßnahmen zu verzahnen und diese jederzeit prüf- und nachweisbar zu dokumentieren.

TopEase setzt genau hier an: Mit einem objekt- und regelbasierten Ansatz bildet die Plattform sämtliche sicherheitsrelevanten Strukturen eines Unternehmens ab. Von Prozessen über Assets bis zu Risiken, Kontrollen und Maßnahmen. So entsteht ein digitales Abbild der Organisation, das Transparenz schafft und gleichzeitig eine belastbare Grundlage für Audits, Reports und Managemententscheidungen bietet.

Digitaler Zwilling als Kernkonzept

Ein zentrales Konzept von TopEase ist der digitale Zwilling der Organisation. In diesem werden alle relevanten Elemente strukturiert erfasst, miteinander verknüpft und bewertet. Abgebildet werden können Prozesse, IT-Systeme, Lieferanten, Standorte, Risiken und Maßnahmen. Durch diese Darstellung lassen sich Abhängigkeiten und Schwachstellen auf einen Blick erkennen:

_____ Welche Systeme sichern kritische Geschäftsprozesse?
_____ Welche Dienstleister sind besonders sensibel?
_____ Wo bestehen regulatorische Risiken?

Über interaktive Diagramme und Dashboards visualisiert TopEase diese Zusammenhänge und liefert damit die Grundlage für fundierte Entscheidungen. Statt isolierter Maßnahmen entsteht eine integrierte Sicht auf Governance, Risiko und Compliance, genauso, wie NIS-2 sie fordert.

Wie TopEase unterstützt

Die Module von TopEase übersetzen die regulatorischen Vorgaben der NIS-2-Richtlinie in strukturiertes Handeln – automatisiert, nachvollziehbar und integriert über alle Ebenen der Organisation hinweg. Alle Module sind integriert und datengetrieben. Änderungen wirken sich automatisch auf verknüpfte Bereiche aus. Das Ergebnis: einheitliche Daten, konsistente Reports und au-

ditfeste Nachvollziehbarkeit. Für die NIS-2-Umsetzung sind besonders folgende Module geeignet:

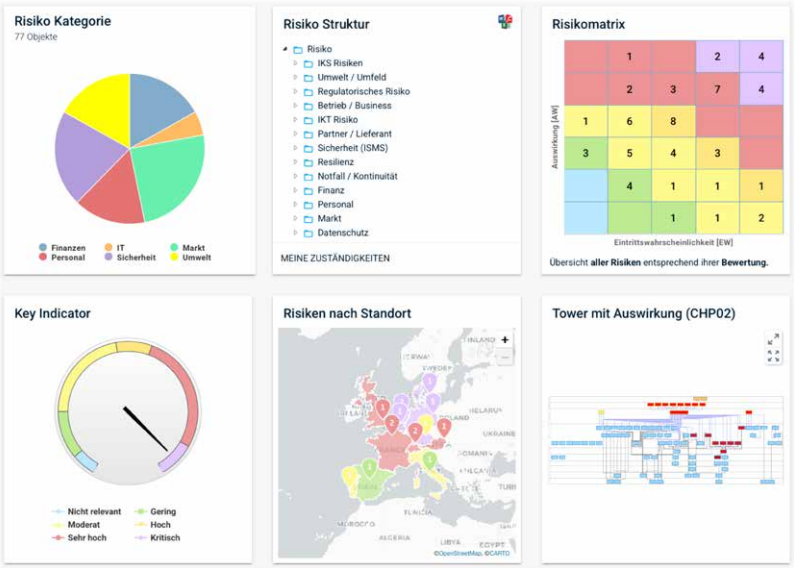
_____ *Sicherheit (ISMS) – Informationssicherheit strukturiert steuern:* Das Sicherheits-Modul von TopEase ermöglicht die systematische Umsetzung von Sicherheitsrichtlinien nach BSI- und ISO-Standards. Schutzbedarfsanalysen, Abweichungsmanagement und automatische Risikoableitungen sorgen für Transparenz und Nachweisfähigkeit – inklusive Statement of Applicability (SOA) und dokumentierter Sicherheitsziele.

_____ *Risikomanagement (NFR) – Risiken erkennen und beherrschen:* Das Risiko-Modul erfüllt die NIS-2-Forderung nach einem nachvollziehbaren Risikomanagementprozess. Risiken werden zentral erfasst, bewertet und mit Prozessen, Assets und Kontrollen verknüpft. Automatisierte Assessments und Risiko-Maps schaffen einen klaren Überblick über Bedrohungslagen und Maßnahmenwirksamkeit.

_____ *Business Continuity Management (BCM/BIA) – Betriebsfähigkeit sichern:* Das BCM-Modul bildet die Anforderungen an Resilienz und Wiederanlaufplanung ab. Prozesse, Systeme und Ressourcen werden end-to-end dokumentiert, BIAs durchgeführt und Notfall-, Wiederanlauf- und Testpläne erstellt. So lässt sich die Betriebs- und Lieferkettenkontinuität gezielt absichern und belegen.

_____ *Drittparteien-Risikomanagement (TPR) – Lieferketten im Blick behalten:* Dieses Modul sorgt für Transparenz und Kontrolle über externe Dienstleister. Es erfasst Lieferanten zentral, bewertet Risiken und Compliance-Standards und überwacht SLAs. Damit unterstützt TopEase die NIS-2-Pflicht, die Sicherheit der gesamten Lieferkette nachweisbar zu gewährleisten.

_____ *Kontrollmanagement (IKS) – Governance und Wirksamkeit sicherstellen:* Unter Kontrollmanagement lassen sich interne Kontrollen dokumentieren, bewerten und regelmäßig prüfen. Über das Prinzip der „Three Lines of Defense“ und integrierte Kontrollmatrizen wird die Wirksamkeit von Sicherheitsmaßnahmen nachgewiesen. Dies ist ein zentraler Bestandteil der NIS-2-Governance-Anforderungen.



Strukturierte Risikoerfassung und -bewertung, ergänzt durch interaktive Dashboards für Analysen, Monitoring und Reporting auf allen Organisationsebenen.

Compliance, die mitdenkt

TopEase ist keine klassische Dokumentationslösung, sondern eine intelligente Steuerungsplattform. Das System prüft automatisch auf Vollständigkeit, steuert Freigaben nach dem Vier-Augen-Prinzip und generiert Benachrichtigungen für Verantwortliche. Die Historienfunktionen sorgt für vollständige Nachverfolgbarkeit. Über integrierte Reporting-Tools lassen sich Auditberichte, Management-Reports und regulatorische Nachweise auf unkompliziert erzeugen. So wird Compliance zu einem dynamischen Prozess, der nicht hemmt, sondern Effizienz und Verantwortlichkeit stärkt.

TopEase unterstützt Single Sign-On (SSO), standardisierte Datenimporte und Schnittstellen-Synchronisationen. Damit fügt sich die Plattform reibungslos in bestehende IT-Infrastrukturen ein. Organisationen behalten die Kontrolle über ihre Datenhoheit und profitieren von zentraler Governance ohne Systembruch.

NIS-2 als Chance für einen integrierten GRC-Ansatz

Die europäische NIS-2-Richtlinie ist ein Katalysator für nachhaltige Informationssicherheit und digitale Resilienz. Mit dem vom Bundeskabinett verabschiedeten NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) nimmt Deutschland Kurs auf eine neue Sicherheitskultur. Weg vom reaktiven IT-Schutz, hin zu integriertem Risikomanagement, klarer Governance und kontinuierlicher Überprüfung.

Auch wenn der Druck bezüglich einer ganzheitlichen Regulierung hinsichtlich Sicherheit und Governance steigt, ist die neue Regulierung eine Chance zur professionellen Modernisierung von Sicherheitsstrukturen TopEase bietet dafür das passende Fundament: strukturierte Datenerfassung, transparente Abhängigkeiten und automatisierte Prozesse in einer Plattform. ■

Angriffserkennung mit der ScanBox

Die Umsetzung der NIS-2-Richtlinie ist oft komplex und ressourcenintensiv. Die ScanBox bietet eine einfache, skalierbare Lösung zur Angriffserkennung. Sie erleichtert die Einhaltung der Vorgaben durch intelligente Analyse und Expertenunterstützung.

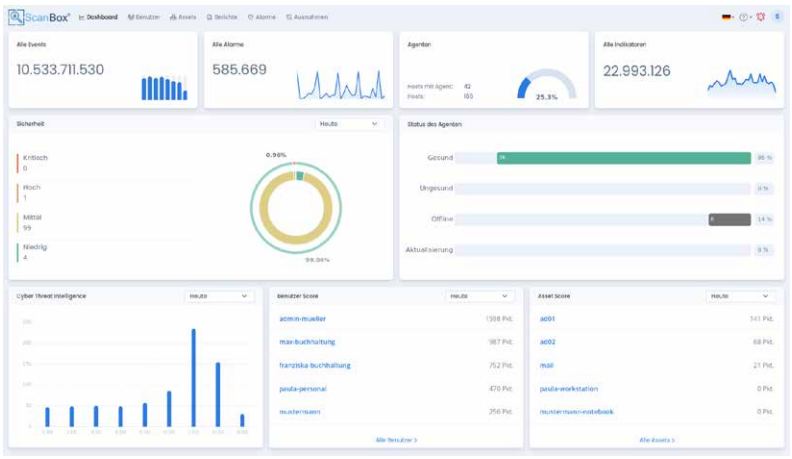
Von Prof. Dr. Kai-Oliver Detken, DECOIT GmbH & Co. KG

Die NIS-2-Richtlinie der Europäischen Union (EU) zur Verbesserung der Cyber- und Informationssicherheit für Unternehmen und Institutionen ist am 17. Oktober 2024 in Kraft getreten. Sie erweitert die Cybersicherheitsanforderungen auf mehr Sektoren und Unternehmen und führt strengere Mindeststandards, Meldepflichten bei Sicherheitsvorfällen sowie höhere Strafen ein für mittlere und große Unternehmen ein, die bestimmte Schwellenwerte bei Mitarbeiterzahl und Umsatz überschreiten. Eine Umsetzung in nationales Recht ist im ersten Quartal 2026 in Deutschland geplant. Spätestens jetzt sollten sich also Unternehmen Gedanken über die Erweiterung ihrer Strategie zur Cybersicherheit machen, um gegen Angriffe von außen und innen sich besser zu schützen oder schlichtweg die Gesetzesvorgaben zu erfüllen.

Zentraler Bestandteil der NIS-2-Richtlinie sind die durchzuführenden Sicherheitsmaßnahmen, die über den bisherigen Stand der Technik hinausgehen. So werden Firewalls als Schutz von äußeren Einflüssen nicht mehr ausreichend angesehen und sollten durch Intrusion-Detection-Systeme (IDS) und Verschlüsselungstechnologien ergänzt werden. Eine kontinuierliche Schwachstellenanalyse sollte durch ein IT-Sicherheitsmonitoring eingeführt werden, um Sicherheitslücken frühzeitig erkennen zu können. Hier kommen sogenannte Security-Information-and-Event-Management-(SIEM) Systeme ins Spiel, die Sicherheitsdaten aus verschiedenen Unternehmensquellen sammeln, analysieren und quasi nahe Echtzeit auswerten. Das Ziel ist es, Bedrohungen und Sicherheitsverstöße frühzeitig zu erkennen, die Einhaltung von Vorschriften zu überwachen und eine schnelle Reaktion zu ermöglichen.

Allerdings fehlt häufig in mittelständischen Unternehmen das entsprechende Fachpersonal, um Sicherheitslücken erkennen und damit umgehen zu können. Dies wird von vielen SIEM-Systemen nicht adressiert. Sie sind für Sicherheitsfachleute in Security Operation Centern (SOC) entwickelt worden. Hinzu kommt, dass meistens nach volumenbasierten Tarifen abgerechnet wird. Das heißt, es wird nach dem tatsächlich anfallenden Datenverkehr der Preis eines solchen Systems ermittelt, wodurch eine feste Planbarkeit der Kosten sich für Unternehmen schwierig gestaltet.

Die DECOIT hat diese Problematik erkannt und ein SIEM-System mit dem Namen ScanBox (https://scanbox-product.de) entwickelt, welches ein einfach zu verstehendes Dashboard für den IT-Systemadministrator enthält und nach der Anzahl der zu überwachenden Assets fest tarifiert wird. Es passt sich daher speichermäßig, als auch preislich der Firmengröße an. Zudem ist es „Made in Germany". Durch die integrierte Cyber-Threat-Intelligence-Korrelation werden aktuelle Bedrohungsdaten genutzt, um verdächtige Muster zu erkennen, Angriffe auszumachen und schnell entsprechende Gegenmaßnahmen einleiten zu können. Auf einen Blick kann so der Administrator erkennen, ob eine problematische Sicherheitslücke vorhanden ist, auf die er sofort reagieren muss, oder die Schwachstellbehebung noch warten kann. Bei technischen Fragen kann er sich nach Bedarf an ein externes SOC wenden, dass die Sicherheitslücke ebenfalls analysiert und ihm Lösungsvorschläge unterbreitet. So ist er gut auf zukünftige Bedrohungen vorbereitet. ■



Das ScanBox Security-Dashboard bietet einen umfassenden Überblick über die IT-Sicherheitslage mit Echtzeit-Kennzahlen zu Events, Alarmen und Agentenstatistiken. (Bild: DECOIT GmbH & Co. KG)

Secupedia – das Portal für Sicherheitsinformationen

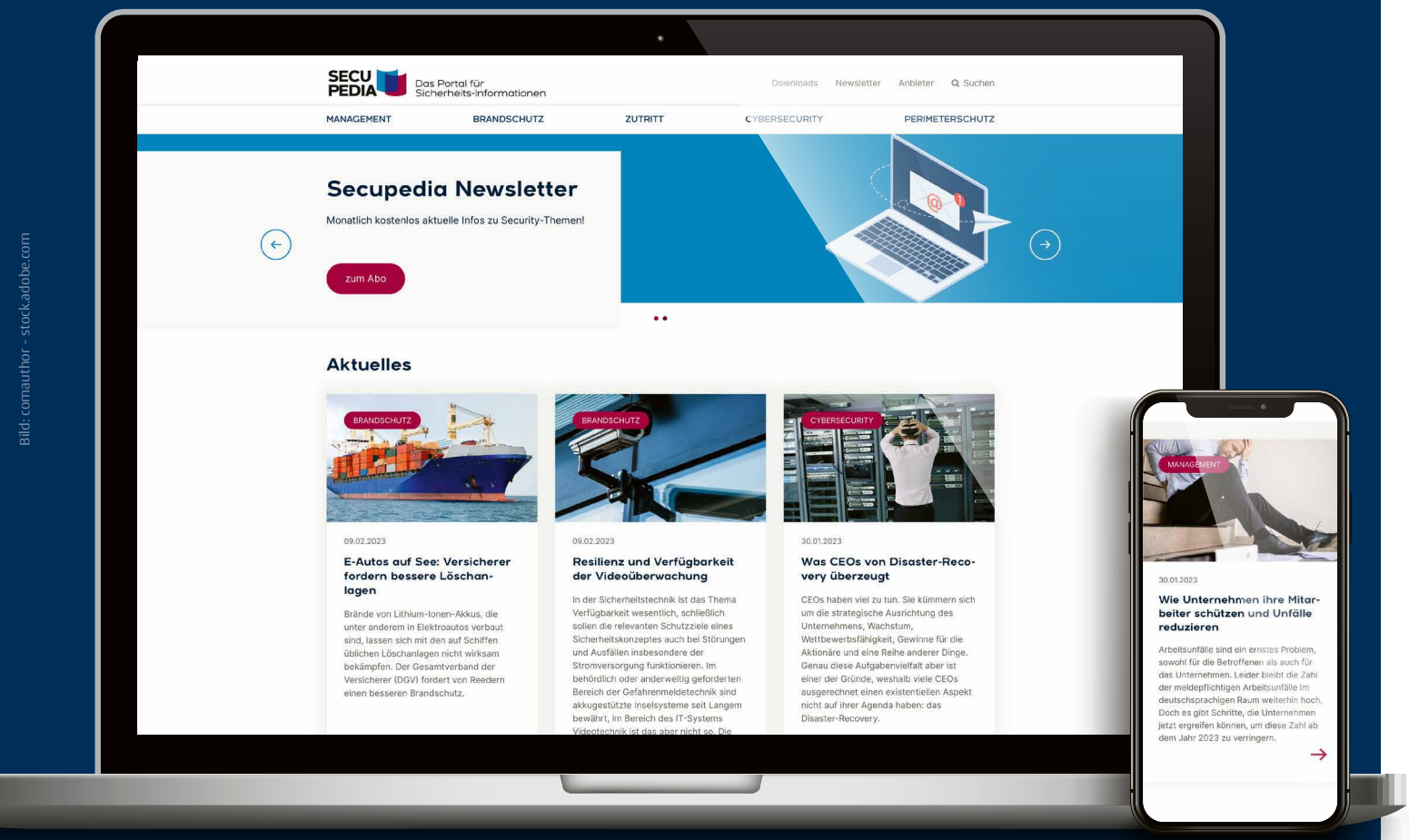


Bild: comauthor - stock.adobe.com

Wir bedanken uns bei unseren Sponsoren:

ARVATO SYSTEMS · BHE · dormakaba · kaspersky

salto INSPIRED ACCESS · sosafe · Synology · TTS trax · zvei electrifying ideas

SECU PEDIA

DATAKONTEXT

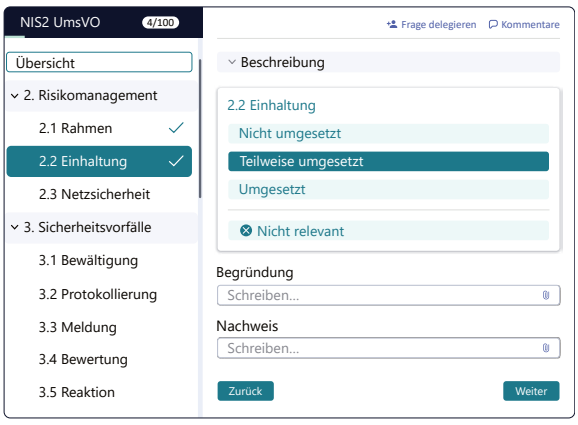
Software ibi systems iris unterstützt Unternehmen bei der NIS-2-Umsetzung

Die ISMS- und GRC-Software ibi systems iris bietet Funktionen zur strukturierten Umsetzung der NIS-2-Anforderungen. Das Tool deckt zentrale Bereiche von der Betroffenheitsprüfung bis zum Risikomanagement ab.

Von Dr. Stefan Wagner, Jad Al-Gaf, Teresa Geiger, ibi systems GmbH

Die Software ibi systems iris hilft Unternehmen dabei, gezielt die Anforderungen der NIS-2-Richtlinie umzusetzen. Sie gewährleistet eine nachvollziehbare Einhaltung gesetzlicher Vorgaben und schafft Transparenz in allen Compliance-Prozessen.

Den Ausgangspunkt hierfür bildet ein integrierter Prüfkatalog des Bundesamtes für Informationssicherheit (BSI) zur Ermittlung der Betroffenheit. Dieser hilft Unternehmen dabei, zuverlässig festzustellen, ob sie unter den Anwendungsbereich der NIS-2-Richtlinie fallen. Ein weiterer Katalog bildet die NIS-2-Umsetzungsverordnung (NIS2 UmsVO) ab, welche die Vorgaben der Richtlinie (Richtlinie (EU) 2022/2555) konkretisiert. Der Prüfkatalog ermöglicht es, die Anforderungen systematisch zu prüfen, Lücken zu identifizieren und die Umsetzung gezielt anzugehen. Damit entsteht eine fundierte Grundlage für die strukturierte Erfassung und Bewertung der Sicherheitsanforderungen sowie für die Steuerung der damit verbundenen Sicherheitsmaßnahmen und Risiken.



Eine dedizierte App für die Prüfungsdurchführung leitet intuitiv durch die Anforderungen mit den vorab definierten Antwortmöglichkeiten. Bei der Beantwortung der Fragen kann eine Begründung sowie ein Nachweis hinterlegt werden. (Bild: ibi systems GmbH)

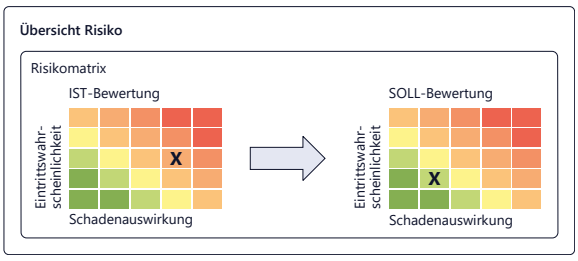
1. Risikomanagement und Maßnahmen

Mit der Software kann der Anwendungsbereich bestehend aus Organisationseinheiten, Assets und Prozessen inkl. Schutzbedarfsfeststellung als Basis für das Risikomanagement abgebildet werden.

Im Rahmen von Prüfungen lassen sich Schwachstellen identifizieren, die zu Risiken führen können. Jedes Risiko erhält eine Kategoriezuordnung und definierte Verantwortlichkeiten. Bei der an die Identifikation anschließenden Risikobewertung werden die Risiken in den Dimensionen Schadenauswirkung und Eintrittswahrscheinlichkeit bewertet und in einer Risikomatrix dargestellt. Dabei ist auch die Einbeziehung weiterer Parameter, wie beispielsweise vergangener Vorfälle, möglich.

Bei der Auswahl der Risikobehandlungsstrategie lassen sich risikomindernde Maßnahmen unmittelbar ableiten und planen. Für eine Maßnahme können zum Beispiel die Wirksamkeit, die Umsetzer sowie das geplante Umsetzungsdatum angegeben werden.

Darüber hinaus lässt sich die Entwicklung der Risiken über die Historie der Risikobewertungen einschließlich der jeweils definierten Maßnahmen nachvollziehen.



Risikoübersicht mit IST- und SOLL-Vergleich (Bild: ibi systems GmbH)

2. Meldepflichten für Sicherheitsvorfälle

Zentral erfasste Vorfälle können per API-Schnittstelle in ibi systems iris übertragen werden. Die Lösung ermöglicht die Aufbereitung und Nachverfolgung der Vorfälle im Rahmen gesetzlicher Meldepflichten. Ferner unterstützt das System direkte Follow-up-Aktivitäten – etwa die Verknüpfung der dokumentierten Vorfälle mit Risiken und Maßnahmen.

3. Betriebskontinuitäts- und -krisenmanagement

Die Grundlage für das Business-Continuity-Management bildet die Erfassung von Assets, kritischen Geschäftsprozessen und Schadensszenarien in ibi systems iris. Mithilfe der Software können strukturierte Business-Impact-Analysen (BIA) durchgeführt und die geforderte Wiederanlaufzeit definiert werden. Die Reportingfunktion erstellt Wiederanlauf- und Wiederherstellungspläne. Notfallereignisse können ebenfalls erfasst und analysiert werden. Aus den Ergebnissen resultierende Risiken werden bewertet und behandelt.

4. Sicherheit der Lieferkette

ibi systems iris bildet vordefinierte oder individuelle Prüfkataloge ab – von internen und externen Audits über Checklisten und Fragebögen bis hin zu Lieferantenprüfungen und Application Security Checks. Die dedizierte App für die Prüfungsdurchführung bindet auch Dritte ein, die ausschließlich Zugriff auf ihre zugewiesenen Prüfungen erhalten. Die Anwendung führt durch die Fragestellungen; Rückfragen werden direkt in der App ohne Medienbruch geklärt.

Prüfungsergebnisse werden über die aus den Ergebnissen resultierenden Maßnahmen, Feststellungen und Risiken nachverfolgt. Da die Elemente eine Verknüpfung zur Prüfung haben, ist jederzeit eine Auswertung pro Prüfung mit dem Status der dazugehörigen Follow-Up-Aktivitäten möglich.

5. Zuweisung von Rollen und Verantwortlichkeiten

Unternehmen können in der Software Rollen definieren und sämtlichen Datensätzen Verantwortlichkeiten zuordnen. Dadurch werden Compliance-Pflichten transparent abgebildet und Verantwortlichkeiten bleiben jederzeit nachvollziehbar.

6. Überwachungen und Audits

ibi systems iris macht es durch weitere Prüfungen und Kennzahlen einfach, sowohl die Maßnahmen als auch die Risiken selbst kontinuierlich zu überwachen und den Maßnahmenstatus zu verfolgen.

Individuell definierbare Automationen und Benachrichtigungsregeln stellen die Umsetzung sicherheitsrelevanter Aufgaben sicher. So kann zum Beispiel die automatische Erstellung von Prüfungen geplant, der Umsetzer einer Maßnahme rechtzeitig vor dem Umsetzungstermin erinnert oder die für ein Risiko verantwortliche Person bei einer anstehenden Neubewertung informiert werden.

Dashboards bieten beispielsweise einen Überblick über Vorfälle, Maßnahmen oder den Grad der Compliance zu Regelwerken. (Bild: ibi systems GmbH)

Vorgefertigte und frei konfigurierbare Reports und interaktive Dashboards tragen ebenfalls zum effektiven Management bei. Beispielsweise liefern Heatmaps zu Risiken, Statusübersichten zu Maßnahmen, Vorfallsübersichten oder Compliance-Cockpits relevante Informationen für Management, Audits oder Behördenmeldungen. Somit werden notwendiger Handlungsbedarf und Verbesserungspotenziale auf einen Blick ersichtlich.

Fazit

ibi systems iris deckt die wesentlichen Anforderungsbereiche der NIS-2-Richtlinie in einer integrierten Lösung ab. Die durchgängige Verknüpfung von Risiken, Maßnahmen, Vorfällen und Prüfungen ermöglicht eine konsistente Dokumentation und erleichtert die Nachweisführung gegenüber Aufsichtsbehörden. Die modulare Struktur erlaubt eine schrittweise Einführung entsprechend den organisationsspezifischen Prioritäten. ■

www.ibi-systems.de

NIS-2: Mehr als eine Checkliste

Warum echte Resilienz jetzt zum entscheidenden Wettbewerbsvorteil wird

NIS-2 ist die Antwort auf systemische Risiken und verlagert die Verantwortung für Cybersicherheit auf die Führungsebene und die gesamte Lieferkette. Als globaler Berufsverband, der Fachkräfte und Organisationen beim Aufbau von digitalem Vertrauen fördert, unterstützt ISACA Unternehmen mit anerkannten Rahmenwerken und der Qualifizierung umfassend geschulter Cybersicherheitsexperten dabei, die weitreichenden Anforderungen der Richtlinie zu erfüllen und die notwendige Kompetenz sowie echte Resilienz aufzubauen.

Von Chris Dimitriadis, ISACA

Die zunehmende Vernetzung globaler Lieferketten und digitaler Ökosysteme ist Fluch und Segen zugleich. Sie steigert die Effizienz, schafft aber auch neue, systemische Risiken. Ein einzelner Ausfallpunkt – ob bei einem Cloud-Anbieter, einem Software-Hersteller oder einem anderen kritischen Dienstleister – kann eine Kettenreaktion auslösen. Die Auswirkungen dieses Phänomens, eine Art digitaler Pandemie, hat die Welt in der jüngsten Vergangenheit mehrfach zu spüren bekommen: Kritische Sektoren wie Kommunikation, Verkehr, Handel und zentrale Arbeitsprozesse wurden dabei weitreichend beeinträchtigt.

Die Konsequenzen – von Produktivitätsverlusten über schwindendes Vertrauen bis hin zu wirtschaftlicher Instabilität – stellen ein allgegenwärtiges Risiko für jedes Unternehmen dar. Cyber-Resilienz darf daher nicht nur eine reaktive Maßnahme sein, sondern muss zum fundamentalen Bestandteil der Infrastruktur und Geschäftsstrategie werden.

Hier setzt die NIS-2-Richtlinie der Europäischen Union an. Sie ist die legislative Antwort auf die neue Risikolandschaft und bietet – richtig interpretiert – Unternehmen einen strategischen Rahmen, um die eigene Widerstandsfähigkeit zu stärken. Dies gilt nicht nur für die Unternehmen der kritischen Infrastruktur, die direkt von NIS-2 betroffen sind, sondern für alle Organisationen, welche die Richtlinie als strategischen Rahmen für ihre Cybersicherheit nutzen.

Verlagerter Fokus

Die Richtlinie verschärft die Sicherheitsanforderungen für Unternehmen und erweitert den Kreis der betroffenen Sektoren. Ziel ist, ein einheitlich hohes Cybersicherheitsniveau in der gesamten EU zu gewährleisten. Zwei Aspekte stehen dabei besonders im Fokus. NIS-2 verankert die Cybersicherheit unmissverständlich auf der Führungsebene. Geschäftsführer und Vorstände sind in der Pflicht, Risikomanagementmaßnahmen für die Cybersicherheit zu überwachen und zu genehmigen. Um strategische Entscheidungen zur Stärkung der Resilienz zu treffen, müssen sie daher die Risikolandschaft aktiv verstehen.

Zudem zeigt die Richtlinie, dass die eigene Resilienz untrennbar mit der Sicherheit der Partner und Dienstleister verbunden ist. Unternehmen werden verpflichtet, die Cybersicherheitsrisiken in ihrer gesamten Lieferkette zu bewerten und zu managen. Dazu gehören eine sorgfältige Auswahl von Lieferanten, die vertragliche Festlegung von Sicherheitsstandards und eine kontinuierliche Überwachung der Partner.

Zwischen Anspruch und Wirklichkeit

Das zentrale Hindernis bei der Umsetzung ist für viele Organisationen die Lücke zwischen den regulatorischen Anforderungen und den verfügbaren Ressourcen. Dies betrifft zum Beispiel den kritischen Mangel an qualifizierten Cybersicherheits-Fachkräften. So geben laut dem „State of Cybersecurity“-Report von ISACA 58 Prozent der europäischen Cybersicherheitsexperten an, dass ihre Teams unterbesetzt sind. Zudem sagen 54 Prozent aus, dass die Budgets für Cybersicherheit in ihrem Unternehmen unterfinanziert sind.

Verschärft wird die Herausforderung durch eine zunehmend komplexe regulatorische Landschaft, in der NIS-2 neben anderen wesentlichen Vorgaben wie DORA und dem AI Act steht. CISOs und die verantwortlichen Führungskräfte müssen jetzt unter hohem Druck die Compliance sicherstellen und gleichzeitig die Ressourcenknappheit navigieren.

Vom Regelwerk zum Wettbewerbsvorteil

Als globaler Berufsverband, der sich seit über 55 Jahren dem Aufbau von digitalem Vertrauen widmet, betrachtet ISACA die NIS-2-Richtlinie als Katalysator für einen überfälligen Wandel. Es geht darum, Cybersicherheit als integralen Bestandteil der Unternehmensstrategie und als Grundlage für digitales Vertrauen zu etablieren – ein Faktor, der zunehmend über den Markterfolg entscheidet. Denn er wird zum direkten Wettbewerbsvorteil: Kunden bevorzugen nachweislich sichere Anbieter und Partner wünschen sich resiliente Glieder in der Lieferkette.

NIS-2 fordert eine integrierte Sicht auf Governance, Risiko und Compliance (GRC), die Silos zwischen IT, Geschäftsleitung und Lieferanten aufbricht. Genau diese Vorgehensweise ist ausschlaggebend, um echte Resilienz zu schaffen. Wenn die Geschäftsführung die Risiken versteht und der CISO die Sprache des Vorstands spricht, können Investitionen gezielt und strategisch getätigt werden: zum Schutz kritischer Prozesse und Aufbau eines vertrauenswürdigen digitalen Ökosystems. NIS-2 ist der Rahmen, der Unternehmen befähigt, diese Transformation strukturiert anzugehen.

Kompetenz als Fundament

Die erfolgreiche Umsetzung von NIS-2 hängt maßgeblich von der nachweisbaren Expertise der verantwortlichen Fachkräfte ab. Die international anerkannten Qualifikationen von ISACA bieten einen weltweit akzeptierten Standard für die Kompetenzen, die für die neuen Anforderungen unerlässlich sind. Sie befähigen Experten unter anderem dazu, Cybersicherheitsstrategien auf Führungsebene zu entwickeln und zu steuern, robuste Governance-Strukturen zu etablieren, komplexe Risiken in der gesamten Lieferkette zu bewerten und zu managen sowie die implementierten Sicherheitsmaßnahmen unabhängig zu prüfen und die Compliance zu belegen.

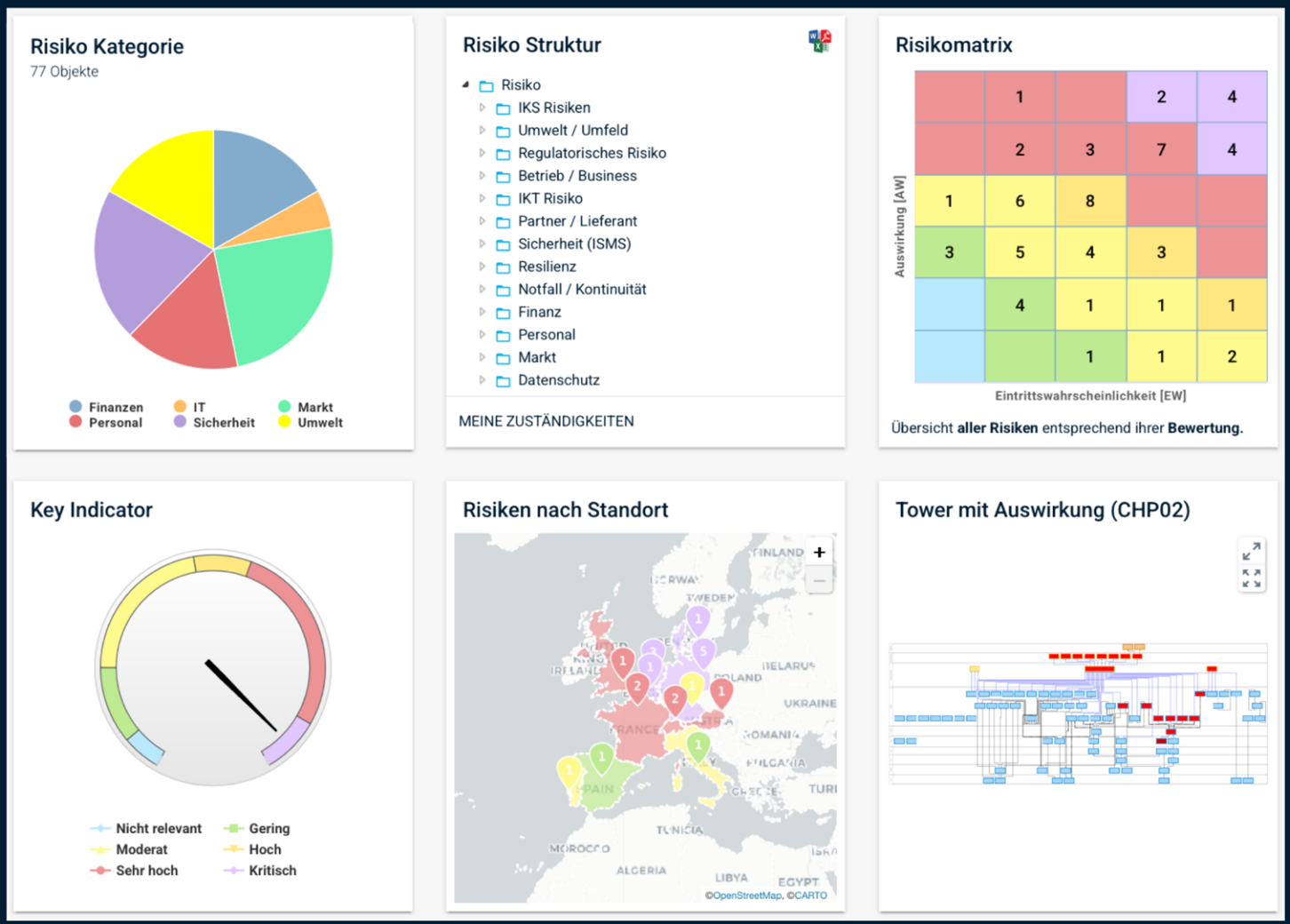
Die Struktur für diese Prozesse liefern international anerkannte Rahmenwerke wie das von ISACA entwickelte Control Objectives for Information and Related Technology (COBIT), das als bewährtes Modell für die IT-Governance dient. Ergänzt wird es unter anderem durch Leitfäden und Whitepaper sowie den Austausch innerhalb der globalen ISACA-Community, der bei der Interpretation neuer Regularien hilft. Durch das Zusammenspiel aus Qualifizierung, strukturierten Rahmenwerken und praxisorientiertem Wissen unterstützt ISACA Organisationen dabei, NIS-2 nicht nur als Pflicht zu erfüllen, sondern als strategische Chance für den Aufbau nachhaltiger Resilienz und eines entscheidenden Wettbewerbsvorteils zu nutzen: digitales Vertrauen.

Der CISO als Architekt der Resilienz

Die erfolgreiche Bewältigung der NIS-2-Anforderungen ist eine Bewährungsprobe für die strategische Reife eines Unternehmens. Sie etabliert den CISO endgültig als Architekten der unternehmerischen Resilienz und löst ihn von der Rolle des technischen Verwalters. Organisationen, die jetzt in die Kompetenz ihrer Fachkräfte investieren, sichern nicht nur ihre Compliance, sondern vor allem ihre Zukunftsfähigkeit in einer zunehmend vernetzten und anfälligen digitalen Welt. ■

TopEASE
ein F24 Produkt

Stärken Sie die Resilienz Ihres Unternehmens – durch einen gesamtheitlichen Blick auf alle Elemente & Zusammenhänge



Schulungspflicht für Top-Manager

Inhalte, Standards und Prüfmaßstäbe nach NIS-2 für die obligatorische Cyberkompetenz von Geschäftsleitungen

Die EU NIS-2-Richtlinie verschärft erheblich die Verantwortung des Top-Managements für Cybersicherheit. Geschäftsleitungen müssen Cybersicherheit als Teil der Unternehmensführung begreifen und sind regelmäßig zu schulen, um Risiken bewerten, Maßnahmen überwachen und gesetzliche Pflichten erfüllen zu können. Der vorliegende Beitrag beschreibt die inhaltlichen, organisatorischen und regulatorischen Anforderungen an solche Management-Schulungen und liefert eine praxisnahe Orientierung, um Cyberkompetenz systematisch zu verankern.

Von Fabian M. Teichmann, St. Gallen (CH)

Die NIS-2-Richtlinie der EU [1] stellt neue Anforderungen an Unternehmen in Bezug auf Cybersicherheit. Erstmals rückt dabei die Verantwortung der Geschäftsleitung stark in den Fokus, weil Führungsgremien (Management-Bodies) Cybersicherheit als integralen Bestandteil der Unternehmensführung etablieren müssen. In Deutschland wird die Richtlinie durch das Mitte November verabschiedete „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (vormals NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, NIS-2UmsuCG) umgesetzt. Bis zum Redaktionsschluss dieser Ausgabe lag allerdings noch keine konsolidierte Fassung des Gesetzestexts vor – zuletzt hatte der Innenausschuss in seiner Beschlussempfehlung [2] noch Änderungen am Entwurf der Bundesregierung [3] vorgeschlagen, die vom Deutschen Bundestag angenommen wurden.

Das neue Gesetz sieht unter anderem in § 38 BSIG-E *„Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen“* vor, dass Geschäftsleitungen regelmäßig geschult werden, um ihren Pflichten bei der Umsetzung und Überwachung von Sicherheitsmaßnahmen gerecht zu werden. Verstöße können zu erheblichen Sanktionen und sogar persönlicher Haftung der leitenden Personen führen. Vor diesem Hintergrund steigt der Druck auf Vorstände* und Geschäftsführer, sich Cyberkompetenz anzueignen. Bereits am 30. September 2025 hat das BSI eine vorläufige Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen [4] nach dem NIS-2-Umsetzungsgesetzentwurf publiziert.

Im Folgenden wird erläutert, welche Inhalte die entsprechenden Schulungen abdecken müssen, wer sie durchführen sollte, wie sich die Wissensvermittlung effektiv gestalten (siehe auch S. 56) und woran sich die Wirksamkeit messen lässt. Ziel ist es, einen strukturierten fachlichen Überblick zu geben, der sowohl Geschäftsführungen, CISOs als auch Aufsichtsbehörden Orientierung bietet.

Erforderliche Schulungsinhalte

NIS-2 verpflichtet das Top-Management, sich ausreichende Kenntnisse und Fähigkeiten in der IT-Sicherheit anzueignen. Der Kerninhalt solcher Schulungen ist das Risikomanagement (vgl. [5]): Führungskräfte sollen lernen, IT-Risiken zu erkennen, zu bewerten und angemessen zu steuern. Tatsächlich betont § 38 Abs. 3 BSIG-E, dass Geschäftsleitungen in die Lage versetzt werden müssen, Risiken und Risikomanagement-Praktiken im Bereich der Informationssicherheit zu identifizieren und zu beurteilen – diese methodische Kompetenz steht im Zentrum.

Darüber hinaus sollten Schulungen für die Geschäftsführung folgende Themenbereiche abdecken:

_____ **Aktuelle Bedrohungslage:** Vermittlung der neuesten Cyberbedrohungen und Angriffsarten, etwa Ransomware, Ausnutzung von Schwachstellen, Supply-Chain-Angriffe et cetera sowie deren potenzielle Auswirkungen auf das eigene Unternehmen (vgl. [6]). Damit wird sichergestellt, dass die Leitung über aktuelle Entwicklungen und Bedrohungen informiert ist und ein Gefühl für die Dringlichkeit von Schutzmaßnahmen entwickelt.

_____ **Grundlagen von Incident-Response und Notfallplanung/Business-Continuity-Management (BCM):** Die Geschäftsleitung sollte wissen, welche Notfall- und Reaktionspläne sowie Krisenmaßnahmen bereitstehen und wie sie im Ernstfall zu aktivieren sind. Dazu gehören Meldewege bei IT-Sicherheitsvorfällen, Kommunikationspläne sowie Zuständigkeiten im Krisenstab. Empfohlen wird auch, das Krisenmanagement regelmäßig in Planspielen oder Simulationen zu üben, damit Entscheider die Abläufe verinnerlichen.

_____ **Einführung in methodisches Risikomanagement – Aufbau eines Informationssicherheits-Risikoprozesses:** Dies umfasst das Identifizieren von schutzwürdigen Gütern und Schwachstellen, Analysieren von Risiken (Bedrohung und Verwundbarkeit), Bewerten von Risiken (z. B. nach Eintrittswahrscheinlichkeit und Schadenshöhe) sowie deren Behandlung durch geeignete Sicherheitsmaßnahmen – die kontinuierliche Überwachung des Risikoprozesses gehört ebenfalls dazu. Ein strukturelles Verständnis versetzt das Management in die Lage, Sicherheitsrisiken angemessen einzuschätzen und priorisierte Entscheidungen zu treffen.

_____ **Überblick über anerkannte Standards und Best Practices der Informationssicherheit,** damit die Führungsebene die eigenen Sicherheitsmaßnahmen im Kontext verorten kann: Dazu zählen beispielsweise die ISO/IEC 27001 (Informationssicherheits-Managementsystem, ISMS) sowie darauf aufbauende Normen wie ISO 27002 (IS-Maßnahmen) und ISO 27005 (Risikomanagement, vgl. Kap. 5 in [7]) oder branchenspezifische Standards. Auch der BSI IT-Grundschutz (www.bsi.bund.de/grundschutz) sowie branchenspezifische Sicherheitsstandards (B3S, www.bsi.bund.de/dok/13099278) sollten erwähnt werden, sofern relevant. Durch diese Orientierung wird verdeutlicht, welche Mindestanforderungen üblich sind und wo das eigene Unternehmen steht. Zudem sollten grundlegende organisatorische und technische Maßnahmen auf „Management-Niveau" (Strategie und Verantwortlichkeiten, keine technische Detailtiefe) besprochen werden – etwa Zugangskontrollen, Backup-Strategien, Patchmanagement, Netzwerksicherheit und Security-Monitoring.

_____ **Rechtliche Pflichten und Haftung:** Die gesetzlichen Verpflichtungen für die Geschäftsleitung nach NIS-2 erfolgen in nationaler Umsetzung durch das eingangs erwähnte Gesetz. § 38 BSIG-E fordert die Billigung und Überwachung von Cyberrisikomanagement-Maßnahmen durch das Leitungsorgan. Den Führungskräften muss klar werden, welche Pflichten sie persönlich treffen – zum Beispiel Schulungspflicht, Pflicht zur Umsetzung angemessener Sicherheitsmaßnahmen oder Meldepflichten bei Incidents (§ 32 BSIG-E) – und welche Konsequenzen drohen, falls sie diese Pflichten vernachlässigen: beispielsweise Bußgelder bis zu 10 Mio. € beziehungsweise 2 % vom Umsatz (§ 65 Abs. 5 BSIG-E) oder persönliche Haftungsansprüche bei grober Pflichtverletzung. Dieses Thema sensibilisiert für die Verantwortlichkeit und schafft Motivation, die zuvor genannten Inhalte ernst zu nehmen. Auch verwandte Rechtsgebiete – etwa der Datenschutz (sowie DSGVO-Bußgelder bei unzureichender Sicherheit, siehe etwa [8] zu Art. 33 DSGVO) – können kurz angesprochen werden, um ein ganzheitliches Verständnis der Compliance-Lage zu vermitteln.

Zur didaktischen Aufbereitung empfehlen Experten – und auch das BSI in seiner ersten Handreichung [4] – eine modulare Gliederung der Schulungsinhalte. Konkret lässt sich der Lehrstoff in Vorbereitungs-, Kern- und Ergänzungsmodule unterteilen: *Vorbereitende Module* liefern der Geschäftsleitung wichtiges Kontextwissen wie Grundbegriffe der IT-Sicherheit, Bedrohungslandschaft oder rechtliche Rahmenbedingungen, um ein gemeinsames Verständnis zu schaffen. Darauf bauen die *Kern-Module* auf, welche die oben genannten zentralen Inhalte vertiefen (Risikomanagement-Prozess, Notfallmanagement, Pflichten). *Ergänzende Module* können schließlich spezifische Themen behandeln, die je nach Unternehmensprofil relevant sind – etwa besondere Branchenrisiken, Fallstudien zu realen Cybervorfällen oder neue Entwicklungen (z. B. Cloud-Sicherheit, Supply-Chain-Risiken oder künstliche Intelligenz, KI).

Durch ein derart modulares Konzept lassen sich Schulungen flexibel an Vorkenntnisse und Bedürfnisse der Teilnehmer anpassen. Das BSI schlägt vor, externe

Standard-Schulungen durch solche unternehmensspezifischen Module zu ergänzen, um Theorie und Praxis zu verzahnen. Die allgemeinen Grundlagen werden also gegebenenfalls von externen Experten vermittelt, während interne Fachleute die Umsetzung im eigenen Unternehmen illustrieren: beispielsweise die Vorstellung der eigenen Notfallprozesse, Richtlinien und bereits umgesetzten Maßnahmen.

Trainings: intern vs. extern

Grundsätzlich kommen für die Durchführung von Schulungen sowohl interne Experten als auch externe Anbieter infrage – oft ist eine Kombination sinnvoll.

Ein internes Schulungsteam könnte etwa der Chief-Information-Security-Officer (CISO) oder IT-Sicherheitsbeauftragte (IT-SiBE) leiten: Interne Experten kennen die spezifischen Geschäftsprozesse, die vorhandene IT-Landschaft und die Unternehmenskultur am besten. Sie können dadurch Schulungsinhalte passgenau auf die eigene Organisation zuschneiden und mit vertraulichen Details arbeiten (etwa interne Risikoberichte oder vergangene Sicherheitsvorfälle). Zudem signalisiert es Engagement, wenn der eigene CISO das Top-Management schult – es entsteht ein direkter Dialog zwischen Führung und Sicherheitsteam.

Allerdings sind nicht alle Unternehmen in der Lage, solche Schulungen eigenständig didaktisch hochwertig aufzusetzen. Hier kommen externe Schulungsanbieter ins Spiel, die auf Management-Schulungen im Bereich Cybersecurity spezialisiert sind. Externe Trainer bringen breitgefächertes Fachwissen und Erfahrung aus vielen Unternehmen mit. Sie können anhand von Best Practices und Branchenvergleichen aufzeigen, wo Handlungsbedarf besteht, und kennen aktuelle Bedrohungen oft aus erster Hand (z. B. aus der Incident-Response-Beratung).

Professionelle Anbieter, etwa von Schulungsakademien oder zertifizierte Trainer, verfügen zudem meist über erprobtes Schulungsmaterial und didaktische Konzepte, die speziell auf Führungskräfte zugeschnitten sind. Nicht zuletzt wird ein externer Nachweis von manchen Aufsichtsbehörden oder Kunden positiver wahrgenommen: Ein offizielles Zertifikat oder eine Teilnahmebescheinigung eines renommierten Schulungsinstituts kann reputationsfördernd sein und im Audit als Beleg dienen.

Die optimale Lösung liegt häufig in einer Mischstrategie: So könnte etwa ein externer Dienstleister ein Grundlagenseminar zu NIS-2-Anforderungen, Bedrohungslage und Risikomanagement-Methodik anbieten, während interne Verantwortliche firmenspezifische Aspekte ergänzen. Tatsächlich hält das BSI es für zweckmäßig, externe Schulungsangebote um unternehmensindividuelle Inhalte zu erweitern, die durch interne Experten vermittelt werden. Beispielsweise könnte nach einem allgemeinen Teil ein interner CISO erläutern, wie das Risikomanagement konkret im eigenen Haus umgesetzt wird, welche Notfallpläne existieren und wo die größten Risiken aus Sicht der Organisation liegen. Eine solche Zusammenarbeit stellt sicher, dass die Schulung sowohl dem allgemeinen Stand der Technik entspricht als auch die individuellen Gegebenheiten berücksichtigt.

Qualifikation der Referenten

Ob intern oder extern, die Lehrenden sollten über umfassende Fachkenntnisse der Cybersecurity verfügen und didaktische Fähigkeiten besitzen. Führungskräfte lernen anders als Techniker, da es weniger um operative Details als um strategische Relevanz, Zusammenhänge und Entscheidungsfolgen geht. Daher sollten Trainer in der Lage sein, komplexe technische Sachverhalte in geschäftsrelevante Sprache zu übersetzen.

Zertifizierungen (z. B. CISM, CISSP, ISO-27001-Trainer) können ein Indikator für Kompetenz sein, sind aber nicht allein entscheidend. Wichtiger sind Erfahrungen in der Kommunikation mit dem Top-Management und idealerweise ein Verständnis der jeweiligen Branche. Im Falle interner Trainer sollte man prüfen, ob eine „Train-the-Trainer"-Weiterbildung sinnvoll ist, um Präsentationstechniken und pädagogische Methoden zu optimieren.

Effektive Wissensvermittlung

Ein zentrales Anliegen ist, dass die adressierten Führungskräfte die vermittelten Inhalte wirklich verstehen und in ihrem Handeln berücksichtigen. Dafür genügt es nicht, sie einmalig mit theoretischen Folien zu „beschallen" – stattdessen sind didaktisch abwechslungsreiche Formate und regelmäßige Auffrischungen gefragt.

Didaktische Aufbereitung

Empfehlenswert sind interaktive Lehrmethoden, die das Top-Management aktiv einbinden: Klassische Frontalvorträge stoßen schnell an Grenzen und Manager schätzen eher praxisnahe und relevante Inhalte. Fallstudien etwa bieten die Möglichkeit, echte Cybervorfälle – möglichst aus ähnlichen Branchen – gemeinsam zu analysieren: Was ist passiert? Welche Entscheidungen hätte das Management treffen müssen? Welche Lehren ergeben sich? Solche Beispiele erhöhen die Aufmerksamkeit und zeigen konkret, warum ein Thema wichtig ist.

Ebenfalls bewährt haben sich Planspiele oder Tabletop-Exercises, in denen man ein simuliertes Szenario

durchspielt. Beispielsweise könnte ein Ransomware-Angriff auf das eigene Unternehmen simuliert werden; Die Geschäftsleitung muss unter Zeitdruck entscheiden, ob Systeme abgeschaltet, externe Stellen informiert oder Lösegeldforderungen adressiert werden. Durch solche Übungen in geschützter Umgebung wird klar, wo noch Unsicherheiten bestehen, und die Führungskräfte lernen durch Erfahrung. NIS-2 fordert explizit, dass das Management Cybersicherheitsrisiken beurteilen kann – auch das gelingt am besten durch kontinuierliches Üben.

Format und Dauer

Die gesetzliche Mindestvorgabe laut Entwurf ist eine Schulung alle drei Jahre für etwa vier Stunden (§ 38 Abs. 3 BSIG-E bzw. Vorgabe 4.2.4 in [3]). Experten halten dieses Intervall für das absolute Minimum – sinnvoll ist es, häufiger und in kleineren Häppchen Wissen zu vermitteln. Beispielsweise könnte jährlich eine kürzere Fortbildung (1–2 Stunden) zu neuen Bedrohungen oder geänderten Compliance-Vorgaben stattfinden sowie alle 2–3 Jahre ein größerer Workshop inklusive Simulationstraining. Auf diese Weise bleibt das Thema präsent und die Inhalte veralten nicht.

Wichtig ist, die verfügbare Zeit der Top-Manager effizient zu nutzen: E-Learning-Module können etwa Grundwissen vorausliefern, sodass die Präsenzzeit für Diskussion und Praxis genutzt wird. Auch Blended Learning – also eine Mischung aus Online-Selbststudium und gemeinsamen Workshops – kann den Wissenstransfer verbessern.

Entscheidend ist, dass nach Abschluss einer Schulung Raum für Fragen bleibt – ein moderiertes Q&A oder Rundengespräch hilft, Unklarheiten auszuräumen und Feedback der Teilnehmer aufzunehmen. So spürt der Trainer, ob die Kernbotschaften angekommen sind – und die Führungskräfte haben Gelegenheit, die Relevanz für ihr Tagesgeschäft zu reflektieren.

Verständnis prüfen

Um sicherzugehen, dass vermitteltes Wissen wirklich verankert ist, bieten sich leichte Kontrollmechanismen an. Das muss kein Examen sein, aber etwa ein kurzes Quiz oder die gemeinsame Bewertung eines Beispielrisikos können Aufschluss über die Erfolge geben.

Manche Organisationen lassen die Teilnehmer am Ende anonym Feedback geben und ein Selbstassessment durchführen: „Wie sicher fühle ich mich nun beim Thema Cyberrisiken?“ Andere führen einige Wochen nach der Schulung einen Follow-up-Termin oder ein Memo mit Schlüsselfragen durch, um das Gelernte aufzufrischen. Solche Maßnahmen fördern die nachhaltige Verankerung.

Wichtig ist zu bedenken, dass Menschen die entscheidenden Faktoren in der Cyberabwehr bleiben (vgl. auch [6]). Schließlich lässt sich auch beobachten, ob und wie sich das Verhalten der Geschäftsführung ändert – etwa ob in Vorstandssitzungen nun regelmäßig Cyberrisiken erörtert werden oder Sicherheitsüberlegungen stärker in Entscheidungsprozesse einfließen. Solche Verhaltensindikatoren deuten darauf hin, dass echtes Verständnis gewachsen ist.

Dokumentation und Nachweis

Von großer Bedeutung – gerade im Hinblick auf Prüfbarkeit – ist die sorgfältige Dokumentation der Schulungen. Jede durchgeführte Maßnahme sollte protokolliert werden – inklusive Datum, Dauer, Teilnehmer, Dozenten und behandelten Inhalten. Empfehlenswert ist beispielsweise das Führen von Teilnahmebescheinigungen oder -listen, die von den Teilnehmern unterschrieben oder digital bestätigt werden (vgl. § 30 Abs. 1 BSIG-E inkl. Erläuterung in [3] sowie Ziff. 3.2 in [4]). Auch die Schulungsunterlagen (Präsentationen, Handouts) sollte man archivieren. All diese Nachweise dienen intern der Qualitätssicherung und gegenüber Aufsichtsbehörden als Beleg der Compliance.

Das BSI betont, dass Geschäftsleitungen durch regelmäßige Schulungen und Awareness-Maßnahmen ihr Sicherheitsbewusstsein schärfen und aktuelle Bedrohungen besser einschätzen können. Zugleich erwartet es eine entsprechende Nachweisführung – das heißt im Falle einer Prüfung muss das Unternehmen zeigen können, dass Führungskräfte tatsächlich wie gefordert geschult wurden. Daher ist es ratsam, die Dokumentation im Rahmen des ISMS vorzuhalten und zum Beispiel in Management-Reviews auf Vorstandsebene das Thema „Schulung der Leitung“ regelmäßig abzuhaken.

Prüfmaßstäbe und Wirksamkeitskontrolle

Die Wirksamkeit von Management-Schulungen lässt sich anhand mehrerer Maßstäbe messen. Zum einen gibt es formale Compliance-Kriterien: Wurden die gesetzlichen Vorgaben (Inhalt, Turnus, Dokumentation) erfüllt? Zum anderen stellt sich die Frage nach der tatsächlichen Wirkung auf das Sicherheitsniveau im Unternehmen. Nachfolgend einige Anhaltspunkte und Standards:

Erfüllung formaler Standards

Unternehmen sollten ihr Schulungsprogramm an etablierten Normen und Rahmenwerken ausrichten: ISO/IEC 27001 fordert zum Beispiel, dass alle rollenbezogenen Kompetenzen entwickelt und erhalten werden – in-

klusive der obersten Leitung. Ein zertifiziertes ISMS nach ISO 27001 impliziert also, dass regelmäßige Schulungen und Awareness-Maßnahmen geplant und umgesetzt werden. Auch der ISO-Standard zum Risikomanagement lässt sich heranziehen (vgl. Kap. 5 Rn. 67 in [7]): Wenn die Geschäftsführung gemäß ISO 27005 die Schritte des Risikomanagements versteht, erfüllt sie zugleich eine NIS-2-Kernforderung.

Branchenspezifische Sicherheitsstandards (B3S), wie sie für KRITIS-Sektoren definiert sind, enthalten ebenfalls Schulungsanforderungen. So schreibt etwa der B3S für die Gesundheitsversorgung regelmäßige Schulungen und Übungen vor, um auf Notfälle vorbereitet zu sein. Solche branchenspezifischen Kataloge werden von Aufsichtsbehörden bei Prüfungen als Benchmark verwendet – sie konkretisieren gewissermaßen die allgemeineren NIS-2-Vorgaben für die jeweilige Branche. Ein Unternehmen, das die für seine Branche geltenden Standards einhält, wird also im Bereich „Management-Schulung" die richtigen Themen abdecken und angemessene Intervalle einhalten.

Anforderungen der Aufsichtsbehörden

Die zuständigen Behörden – in Deutschland vor allem das BSI als zentrale Stelle für Cyber-Sicherheit – achten im Rahmen von Audits oder Nachweisanforderungen auf dieses Thema. Gemäß nationalem NIS-2-Umsetzungsgesetz müssen kritische Einrichtungen alle drei Jahre ein Audit vorlegen, während für wichtige Einrichtungen Stichprobenprüfungen vorgesehen sind (§§ 30 und 39 Abs. 1 BSIG-E).

Im Auditfall wird geprüft, ob das Top-Management seinen Pflichten nachkommt – hier wird das Vorhandensein eines Schulungskonzepts und der entsprechenden Teilnahmenachweise verlangt (§ 39 Abs. 1 Satz 3 BSIG-E). Das BSI kann zum Beispiel anordnen, Nachweise über die Erfüllung aller Anforderungen vorzulegen – fehlende Schulungsnachweise würden dann als Compliance-Verstoß gewertet.

Entsprechend sollten Unternehmen darauf vorbereitet sein, einer Aufsichtsbehörde zum Beispiel ein Schulungskonzept oder eine Policy vorzulegen, aus denen Inhalte, Dozenten, Frequenz und Dokumentation hervorgehen. Auch Auditoren – etwa ISO-27001-Prüfer oder die interne Revision – werden gezielt fragen, wie die Geschäftsführung in das Sicherheitsmanagement eingebunden ist und ob sie geschult wurde. Ein positives Signal ist, wenn das Top-Management selbst in Audit-Interviews grundlegende Cybersecurity-Begriffe korrekt verwendet und die firmenspezifischen Top-Risiken benennen kann – dies deutet auf eine gelungene Sensibilisierung hin.

Interne Erfolgskontrolle

Auch über die reine Compliance hinaus sollte jedes Unternehmen selbst evaluieren, ob Schulungen den gewünschten Effekt haben. Hierfür bieten sich sowohl qualitative als auch quantitative Ansätze an.

Qualitativ lassen sich Feedback-Runden nutzen, in denen Führungsmitglieder anonym Rückmeldung geben, ob die Schulung für sie verständlich und relevant war, und wo sie noch Unsicherheiten sehen. Diese Rückmeldungen sollte man ernst nehmen und das Schulungskonzept kontinuierlich verbessern (Stichwort PDCA-Zyklus im ISMS).

Quantitativ könnte man bestimmte Kennzahlen verfolgen – dies ist jedoch schwieriger, da der Erfolg von Cybersicherheit nicht leicht messbar ist. Dennoch: Man könnte zum Beispiel tracken, ob sich die Anzahl kritischer Sicherheitsvorfälle im Zeitverlauf ändert (weniger erfolgreiche Angriffe nach intensiver Schulung der Leitung?) oder ob Investitionsentscheidungen zugunsten der IT-Sicherheit zunehmen – das würde zeigen, dass das Management deren Wichtigkeit erkannt hat. Auch Ergebnisse von Phishing-Tests in der Belegschaft könnten indirekt beeinflusst werden: Wenn die Geschäftsführung Cybersicherheit vorlebt, steigt oft die Sicherheitskultur insgesamt. Letztlich bleibt die Kulturveränderung ein weicher, aber wichtiger Indikator: Spricht das Management in Strategie-Meetings nun aktiv Risiken an? Fordert es von Fachabteilungen Berichte zur Cyberlage ein? So etwas lässt sich zum Beispiel in Management-Protokollen oder Risiko-Workshops beobachten.

Audits und Reviews

Eine weitere sinnvolle Maßnahme sind interne Audits speziell zum Schulungsthema. Die interne Revision oder ein externer Auditor könnten prüfen, ob Schulungsmaterialien aktuell sind, die Führungskräfte (falls durchgeführt) die Tests bestanden haben und ob Folgemaßnahmen aus dem Feedback umgesetzt wurden. Zusätzlich könnten Simulationen (wie schon erwähnt) nicht nur als Training, sondern auch als Reifegrad-Check dienen: Wird ein Übungsszenario deutlich souveräner bewältigt als eine frühere Übung vor ein, zwei Jahren, spricht das für einen Lerneffekt. Diese Fortschritte sollte man dokumentieren.

Gegebenenfalls kann man auch Zertifizierungen in Betracht ziehen: Es gibt mittlerweile Trainingszertifikate für Manager im Bereich Cybersecurity (auch wenn die Qualität variiert). Solche Zertifikate, zum Beispiel Teilnahmebestätigungen von TÜV-Seminaren oder Ähnliches,

können in die Personalakten der Geschäftsführer aufgenommen und gegenüber Gesellschaftern oder Aufsichtsräten kommuniziert werden, um Vertrauen zu schaffen.

Fazit

Die Schulung des Top-Managements in Sachen Cybersicherheit ist kein Nice-to-have, sondern eine Pflichtaufgabe nach NIS-2, die mit Augenmaß und Strategie angegangen werden muss.

Geschäftsführungen müssen in regelmäßigen Abständen – mindestens alle drei Jahre, eher häufiger – Trainings absolvieren, die ihnen helfen, die digitale Bedrohungslage zu verstehen und informierte Entscheidungen zu treffen. Inhaltlich stehen Risikomanagement und Notfallvorsorge im Mittelpunkt, eingebettet in einen Überblick über aktuelle Gefahren und Compliance-Anforderungen. Durch entsprechende Standards (ISO 27001 u. a.) sowie behördliche Vorgaben ist ein Rahmen abgesteckt, innerhalb dessen Organisationen ihre Lösungen finden können.

Ob Schulungen intern, extern oder gemischt durchgeführt werden, hängt von den Möglichkeiten des Unternehmens ab. Wichtig ist in jedem Fall, dass Praxisbezug und Interaktivität gegeben sind, damit der Lerntransfer gelingt. Die Wirksamkeit zeigt sich letztlich daran, dass das Management seiner Rolle gerecht wird, Cybersicherheit als Chefsache begreift und aktiv in die Unternehmensführung integriert.

Werden Schulungsmaßnahmen konsequent geplant, durchgeführt und nachverfolgt, lässt sich nicht nur der gesetzlichen Nachweispflicht genügen, sondern vor allem ein höheres Schutzniveau für die gesamte Organisation erreichen. Eine Investition in Cyberkompetenz im Vorstand zahlt sich aus: in Form informierter Entscheider, geringerer Risikoexposition und letztlich einer resilienten, vertrauenswürdigen Geschäftstätigkeit im digitalen Zeitalter. ■

Dr. iur. Dr. rer. pol. Fabian M. Teichmann, LL.M. (London), MBA (Oxford) ist Rechtsanwalt und Notar sowie Managing Partner der Teichmann International (Schweiz).

Literatur

[1] Europäische Union, Richtlinie (EU) 2022/2555 ... vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, ... (NIS-2-Richtlinie), konsolodierte Fassung, Dezember 2022, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02022L2555-20221227

[2] Deutscher Bundestag – Innenausschuss, Beschlussempfehlung und Bericht zu dem Gesetzentwurf der Bundesregierung – Drucksachen 21/1501, 21/2072, 21/2146 Nr. 1.11, BT Drucksache 21/2782, November 2025, https://dserver.bundestag.de/btd/21/027/2102782.pdf

[3] Deutscher Bundestag, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Gesetzentwurf der Bundesregierung, BT Drucksache 21/1501, September 2025, https://dserver.bundestag.de/btd/21/015/2101501.pdf

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), NIS-2-Geschäftsleitungsschulung, Vorläufige Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen nach dem NIS-2-Umsetzungsgesetzentwurf, Version 0.9, September 2025, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf

[5] Fabian M. Teichmann, NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) – neue Pflichten für Länder- und Kommunalverwaltungen, LKV – Landes- und Kommunalverwaltung 2025/6, Juni 2025, S. 253, https://beck-online.beck.de/?vpath=bibdata%2Fzeits%2FLKV%2F2025%2Fcont%2FLKV%2e2025%2eH06%2ehtm (kostenpflichtig)

[6] Fabian M. Teichmann, NIS-2 in der Energiewirtschaft: Pflichten und Haftungsregime für KRITIS-Betreiber, EnWZ – Zeitschrift für das gesamte Recht der Energiewirtschaft 2025/7, Juli 2025, S. https://beck-online.beck.de/?vpath=bibdata%2Fzeits%2FENWZ%2F2025%2Fcont%2FENWZ%2e2025%2eH07%2ehtm (kostenpflichtig)

[7] Dennis-Kenji Kipker (Hrsg.), Cybersecurity, C. H. BECK, 2. Auflage, Juni 2023, ISBN 978-3-406-79263-2

[8] Peter Gola, Dirk Heckmann (Hrsg,), DS-GVO/BDSG – Datenschutz-Grundverordnung Bundesdatenschutzgesetz, C. H. BECK, 3. Auflage, Oktober 2022, ISBN 978-3-406-78266-4