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-

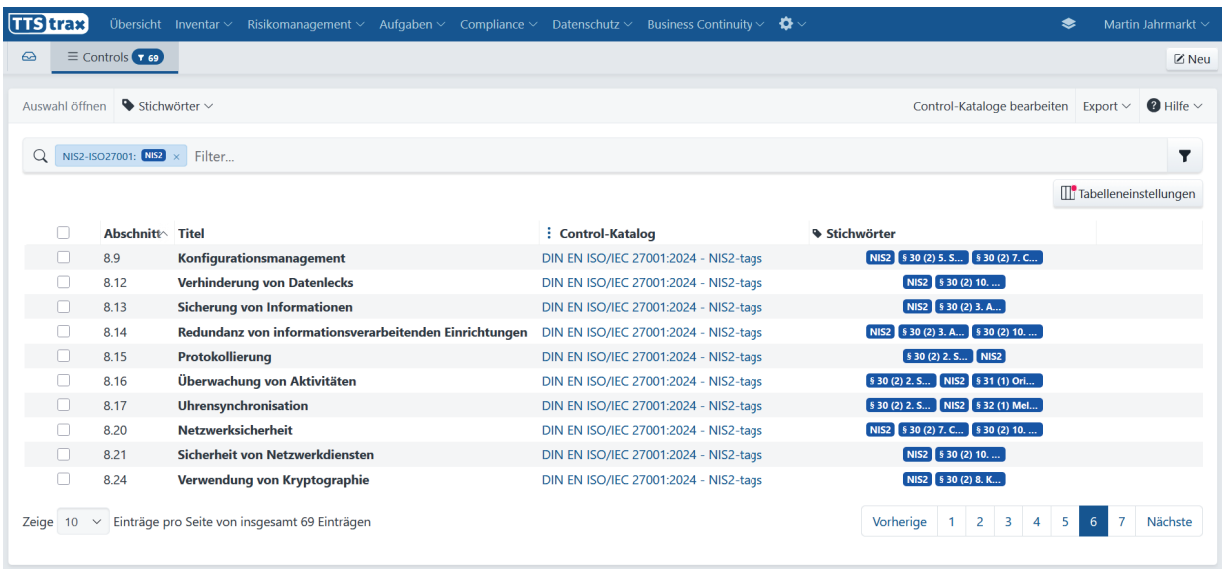

Abbildung 1: Mapping zwischen ISO/IEC 27001-Controls und NIS-2-Anforderungen über Stichwörter-Funktion in TTS trax. (Bild: TTS Trusted Technologies and Solutions GmbH)

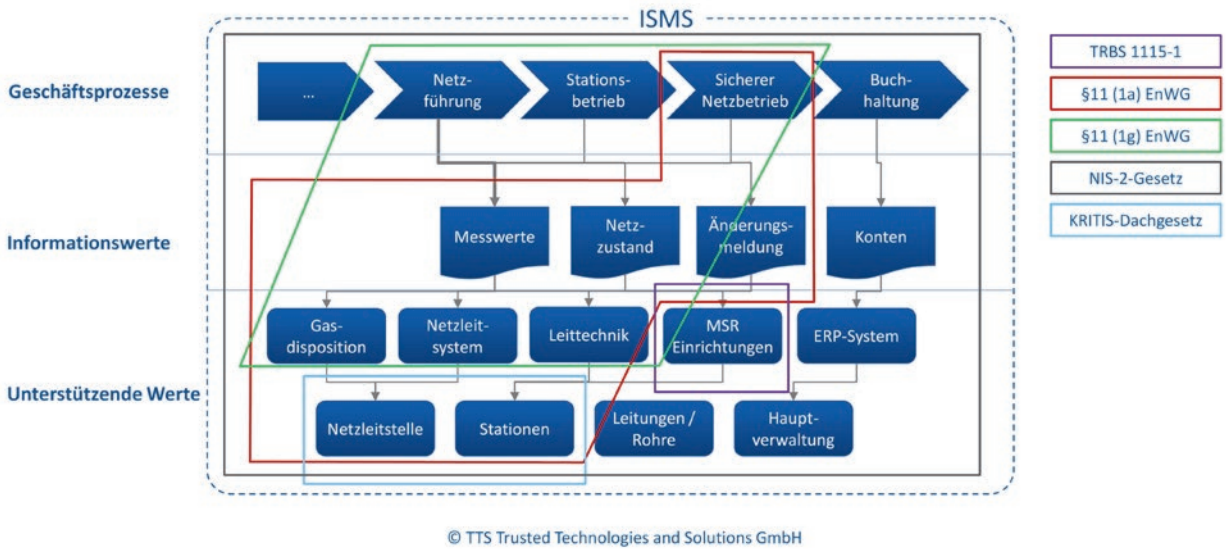

Abbildung 2: Multi-Scope am Beispiel eines Energienetzbetreibers. (Bild: TTS Trusted Technologies and Solutions GmbH)

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:

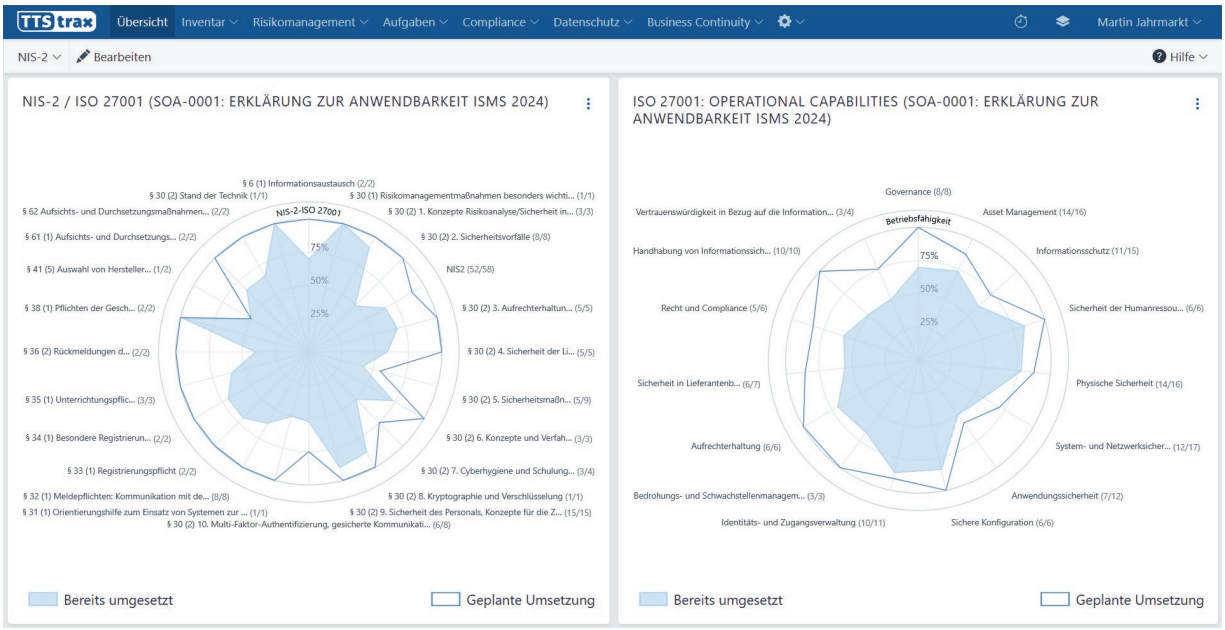

Abbildung 3: Gegenüberstellung von NIS-2-Konformität und ISO/IEC 27001-Umsetzung in TTS trax (Bild: TTS Trusted Technologies and Solutions GmbH)

_____ 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. ■