NIS2: Von der Compliance-Last zum Katalysator

Die intrinsische Motivation für Informationssicherheit

Unternehmen müssen investieren und innovative Technologien einsetzen, um ihre IT-Infrastruktur vor Cyberangriffen zu schützen. Regulatorische Anforderungen wie NIS2 sollten nicht als Last, sondern als Chance gesehen werden.

Jede Organisation besitzt Werte, die es zu schützen gilt – sei es geistiges Eigentum, Kundendaten, (Produktions-) Prozesse oder ganz allgemein die eigene Wertschöpfung. Der Schutz dieser Werte spiegelt sich in den Grundpfeilern der Informationssicherheit wider: Vertraulichkeit, Integrität und Verfügbarkeit. Dabei handelt es sich nicht um abstrakte Konzepte, sondern um essenzielle Voraussetzungen für den Geschäftserfolg, insbesondere in einer hochdigitalisierten Welt. Gelangen sensible Informationen in falsche Hände, werden Daten manipuliert oder fallen kritische Systeme aus, kann nicht nur erheblicher finanzieller Schaden entstehen, sondern auch die Reputation massiv leiden. Beispiele hierfür finden wir nahezu in täglichen Nachrichtenmeldungen. Der Schutz dieser Werte sollte also eine Selbstverständlichkeit sein.

Paradoxerweise wird der Schutz der eigenen Werte und Prozesse – der eigenen Wertschöpfung – erst dann priorisiert, wenn Regulierungen (wie zum Beispiel die NIS2-Richtlinie) dies einfordern oder ein Informationssicherheitsvorfall eintritt. Dies wirft zwangsläufig die grundlegende Frage auf:

»Wer war als Erstes da: NIS2 oder die Notwendigkeit, seine eigene Organisation zu schützen?«

Die Antwort ist offensichtlich: Die Notwendigkeit seine eigene Organisation zu schützen bestand schon immer – die Regulierung macht sie nun für die betroffenen Unternehmen verbindlich und fordert Nachvollziehbarkeit. Dennoch werden regulatorische Anforderungen oftmals als bürokratische Last wahrgenommen, als extern aufgezwungene Pflicht, die Ressourcen bindet. Diese Sichtweise verkennt den eigentlichen Zweck:

»...Geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ..., um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit von informationstechnischen Systemen, Komponenten und Prozessen, ... zu vermeiden oder die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.« (Art. 30 Abs. 1 des Regierungsentwurfs zum NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz vom Juli 2024 (im Folgenden: NIS2-UmsCyberSG-E)) [1].

Die Diskrepanz zwischen der wahrgenommenen Last der Compliance und dem tatsächlichen Sicherheitsgewinn ist ein Trugschluss, der überwunden werden muss, um Informationssicherheit als strategischen Enabler zu begreifen [2].

Aktueller Stand zu NIS2. Der Rechtsakt zu NIS2 wurde als Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union formuliert und erfordert daher eine Umsetzung in den einzelnen EU-Mitgliedstaaten. Die Frist hierfür war der 17. Oktober 2024 – ein Termin, den viele EU-Staaten, einschließlich Deutschland, nicht eingehalten haben. In Deutschland verhinderte die vorgezogene Bundestagswahl den Abschluss des Gesetzgebungsverfahrens; das Diskontinuitätsprinzip griff ein [3]. Wann das deutsche Umsetzungsgesetz in Kraft tritt und welche Inhalte es final umfassen wird, bleibt unklar. Die mediale Berichterstattung lässt jedoch hoffen, dass noch 2025 Bewegung in die Sache kommt.

Viele Organisationen fragen sich, ob bereits ausreichend belastbare Informationen vorliegen, um sich als potenziell betroffene Organisation auf NIS2 vorzubereiten. Für potenziell nicht betroffene Organisationen stellt sich zudem die Frage, ob man sich daran orientieren sollte. Die erste Frage lässt sich mit einem klaren JA beantworten, wobei

Illustration: © Jozef Micic | Dreamstime.com

*/ Die NIS2-Richtlinie sollte nicht als regulatorische Bürde, sondern als Chance für notwendige Veränderungen und als Anstoß für ein neues Mindset betrachtet werden, das den Schutz der eigenen Organisation priorisiert.

die zweite Frage kritisch zu hinterfragen ist, in Anbetracht diverser, bereits existierender und praktizierter Standards. An die derzeitige, solide Informationslage (Art. 30 NIS2-UmsCyberSG-E / Art. 21 RL (EU) 2022/2555) und die klare Bejahung der ersten Frage schließt sich zugleich die Frage nach dem »Und wie?« an.

NIS2 als Chance für tatsächlichen Sicherheitsgewinn. Um die NIS2-Anforderungen nicht nur abzuhaken, sondern einen echten Sicherheitsgewinn zu erzielen, empfiehlt sich ein ganzheitlicher Ansatz, der über bloße Compliance hinausgeht. Die eingangs erwähnte Diskrepanz zwischen Wahrnehmung und Mehrwert von Compliance-Maßnahmen unterstreicht die Notwendigkeit strategischen und nachhaltigen Handelns [2].

Dieser Ansatz umfasst zwei Perspektiven: den systematischen Umsetzungszyklus und die organisatorischen sowie technologischen Maßnahmen. Der Zyklus besteht aus Kontexterfassung (»Warum?« und »Was?«), Risikomanagement (»Welche Risiken?« und »Wie schützen?«) und Wirksamkeitsbewertung (»Wo Potenziale/Defizite?« und »Wie nachsteuern?«). Diese Fragen steuern den Prozess und fördern die kontinuierliche Verbesserung – ein Prinzip bekannter Standards.

Die organisatorischen und technologischen Maßnahmen selbst sind in der RL (EU) 2022/2555, leider auch im letzten NIS2-UmsCyberSG-E, oberflächlich beschrieben, lassen sich dennoch in etablierte Rahmenwerke und Standards wie das NIST Cybersecurity Framework (CSF) oder die ISO/IEC 27001 (Version 2024) einordnen (Phasen »Identify«, »Protect«, »Detect«, »Respond« und »Recover«). Dies erleichtert die Umsetzung und bringt weitere positive Effekte.

Für eine zielgerichtete und ressourcenschonende Umsetzung empfiehlt sich ein vierstufiges Vorgehen, das den PDCA-Zyklus mit konkreten Maßnahmen verknüpft:

Stufe 1: »Sicherheitskompass«.

Der Einstieg beginnt mit der Zusammenführung aller relevanten Stakeholder – von der Geschäftsführung bis zu verantwortlichen Fachspezialisten. Ziel ist es, zentrale Fragen zu klären und sich auf ein gemeinsames Ziel zu verpflichten: Warum betreiben wir Informationssicherheit? Welche Werte, Prozesse oder Daten sind besonders schützenswert? Welche externen Einflüsse, etwa regulatorische oder geschäftliche Anforderungen, sind zu berücksichtigen? Ein Workshop – gegebenenfalls extern moderiert – kann diese Fragen beantworten, strategische Sicherheitsziele definieren und die Basis für die weitere Vorgehensweise schaffen. Diese Ziele sollten Compliance-Anforderungen ebenso wie geschäftliche Prioritäten und die Verbesserung der Informationssicherheit widerspiegeln und könnten etwa auf eine ISO/IEC 27001-Zertifizierung abzielen, um einen Wettbewerbsvorteil zu erzielen.

Stufe 2: Standortbestimmung mit Möglichkeit zur individuellen Gestaltung.

Die zweite Stufe umfasst eine detaillierte Bewertung des aktuellen Sicherheitsniveaus, idealerweise durch externe Experten mit unvoreingenommenem Blick. In der Analyse werden Abweichungen zwischen dem Ist-Zustand und den aufgestellten Anforderungen und Zielen aus dem initialen Workshop »Sicherheitskompass« identifiziert sowie bestehende Schwachstellen und Risiken aufgedeckt.

Je nach Bedarf können Analysen und Betrachtungen des aktuellen Sicherheitsniveaus in unterschiedlicher Art und Ausprägung erfolgen, um auch die individuellen Bedürfnisse und die gesetzten Ziele zu erfüllen:

- **Quick Check:** Überblicksebene zur Identifikation von Handlungsfeldern (Interview-basiert).
- **Reifegradanalyse:** Detaillierte Bewertung anhand von Konzepten, Dokumentationen und Nachweisen.
- **IT-Grundabsicherung:** Technische Analyse bis auf Konfigurationsebene, für verschiedene Bausteine (etwa AD und PKI).
- **Risikoanalysen und Penetrationstests:** Gezielte Untersuchung kritischer Systeme (»Kronjuwelen«)

Die Ergebnisse liefern ein klares Bild der aktuellen Risikoexposition und bilden die Basis für eine fundierte Roadmap und gezielte Maßnahmen.

Stufe 3: Umsetzungsplanung

Basierend auf der Analyse wird eine priorisierte Strategie entwickelt. Maßnahmen werden nach Risiko, Aufwand und Relevanz gewichtet, um mit begrenzten Ressourcen maximale Wirkung zu erzielen. Die Roadmap kombiniert kurzfristige »Quick Wins« mit langfristigen Initiativen, um das Sicherheitsniveau nachhaltig zu steigern.

Stufe 4: Umsetzung und kontinuierliche Verbesserung

Die priorisierten Maßnahmen werden umgesetzt, begleitet von einem kontinuierlichen Monitoring. Regelmäßige Überprüfungen und Anpassungen gewährleisten, dass die

Ein holistischer Sicherheitsansatz unterstreicht die Notwendigkeit strategischen und nachhaltigen Handelns. Dieser Ansatz umfasst zwei Perspektiven: den systematischen Umsetzungszyklus und die organisatorischen sowie technologischen Maßnahmen.

Sicherheitsarchitektur dynamisch auf neue Bedrohungen und Anforderungen reagiert – ein selbstverstärkender Verbesserungsprozess entsteht.

NIS2 als Katalysator für Wandel und Innovation. Die NIS2-Richtlinie sollte nicht als regulatorische Bürde, sondern als Chance für notwendige Veränderungen und als Anstoß für ein neues Mindset betrachtet werden, das den Schutz der eigenen Organisation priorisiert. Die derzeitige Situation bietet die Chance, Informationssicherheit strategisch neu zu positionieren und von einer reaktiven Pflichtübung zu einem proaktiven Wettbewerbsvorteil zu entwickeln. Eine durchdachte Sicherheitsstrategie und eine robuste Sicherheitsarchitektur schaffen langfristige Vorteile: Sie stärken das Vertrauen von Kunden und Partnern, reduzieren Ausfallzeiten und Schadensfälle und ermöglichen die sichere Nutzung neuer Technologien. Organisationen, die jetzt proaktiv handeln, werden nicht nur compliant sein, sondern die digitale Transformation sicherer und erfolgreicher gestalten.

Controlware – Kompetenter Partner im Bereich GRC. Als IT-Dienstleister und Managed Service Provider unterstützt Controlware Unternehmen und Behörden rund um die Themen Informationssicherheit, IT-Notfallmanagement und IT-Compliance.

Ob es sich um die Realisierung regulatorischer Anforderungen, die Einführung von Managementsystemen (beispielsweise nach ISO27001) oder um die Vorbereitung der Organisation auf entsprechende Zertifizierungen handelt – die Experten von Controlware verfügen über langjährige Praxiserfahrung und themenübergreifendes Fachwissen. Darüber hinaus wird das Leistungsangebot durch tiefgreifende Kompetenz aus den Bereichen Network Solutions, Collaboration, Information Security, Application Delivery, Data Center & Cloud sowie durch spezialisiertes IT-Management und umfangreiche Managed Services komplettiert.

Daniel Kammerbauer,
Team Lead Governance, Risk & Compliance,
Controlware GmbH

www.controlware.de
blog.controlware.de

[1] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html

[2] https://www.veeam.com/de/company/press-release/90-percent-of-emea-businesses-faced-cybersecurity-incidents-that-nis2-could-have-prevented-veeam-survey-reveals.html

[3] https://www.bundestag.de/services/glossar/glossar/D/diskont-245382