NIS-2: Orientierung statt Bürokratie

Interview mit Andreas Grau und Bernhard Schmid von Juliana Lofink

Die neue EU-Richtlinie NIS-2 verunsichert viele Unternehmen: komplexe Vorgaben, knappe Ressourcen, hoher Druck. Wie gelingt ein pragmatischer Start, ohne den operativen Alltag auszubremsen? Und wie können Wirtschaftsprüfer Orientierung geben? Andreas Grau (Consileon) und Bernhard Schmid (4IoT) erklären, welche Maßnahmen sofort wirken und wie NIS-2 in der Unternehmensführung verankert werden kann.

NIS-2 gilt vielen als komplex und bürokratisch. Was ist Ihr wichtigster Rat, um den Einstieg pragmatisch zu gestalten – ohne in Papierarbeit zu versinken?

Grau: Früh Struktur schaffen! Eine kompakte Übersicht über wirklich kritische Prozesse verhindert, dass man sich in Detailanforderungen verliert. Anschließend werden Rollen geklärt und wenige, klar begründete Schritte priorisiert. Dokumentation bleibt wichtig, sollte aber ausschließlich Entscheidungen, Risiken und das Vorgehen nachvollziehbar machen. So entsteht ein klarer Rahmen, der den Einstieg erleichtert.

Schmid: Der wichtigste Rat ist es, NIS-2 konsequent risikobasiert und verhältnismäßig umzusetzen. Verhältnismäßig heißt, sich auf die wenigen wirklich relevanten Risiken zu konzentrieren und sie schlank zu dokumentieren. So erfüllt man die Anforderungen ohne unnötige Bürokratie.

Lassen Sie uns konkret werden, Herr Schmid. Wenn ein Unternehmen morgen starten muss: Welche drei Sofortmaßnahmen bringen schnell Ordnung und Sicherheit – mit realistischem Aufwand?

Ein schneller Einstieg gelingt über drei Schritte. Erstens Transparenz schaffen mit einem einfachen Risikoregister mit den geschäftskritischen Informationswerten, wie Geschäftsprozesse, IT-Systeme, Dienstleister und grundsätzlichen Risiken. Bewertung und abgeleitete Maßnahmen werden dort dokumentiert. Diese einfache Bestandsaufnahme zeigt unmittelbar, wo Handlungsbedarf besteht. Zweitens Maßnahmen stärken, die die häufigsten Angriffswege schließen – etwa Multi-Faktor-Authentifizierung, konsequentes Patchen und verlässliche Backups. Drittens ein schlanker Ablauf für Sicherheitsvorfälle, damit Risiken nicht nur erkannt, sondern auch kontrolliert werden können. Das schafft einen unmittelbaren, wirksamen Einstieg.

Wie gelingt es, dass NIS-2 nicht als IT-Sache abgetan wird, sondern als Managementaufgabe gelebt wird – mit klaren Zuständigkeiten und Entscheidungen?

Grau: Der Schlüssel ist ein Lagebild über die Wertschöpfung des Unternehmens mit externen Anforderungen und realistischen Störungsszenarien. Damit wird verständlich, warum NIS-2 strate-

NIS-2

Die NIS-2-Richtlinie ist eine EU-Vorgabe zur Stärkung der Cyber- und Informationssicherheit und verschärft die Anforderungen an Unternehmen zur Erhöhung ihrer Widerstandsfähigkeit gegenüber Cyberrisiken. Sie ist seit Januar 2023 in Kraft. In Deutschland erfolgte die Umsetzung über das neue BSI-Gesetz.

Für Wirtschaftsprüfer gewinnen damit Governance, Entscheidungs- und Wirksamkeitsaspekte von Cyber- und IT-Risiken in Prüfung und Beratung deutlich an Bedeutung.

Perfektionismus kann hinderlich sein, wenn es darum geht, eine Aufgabe zeitgerecht zu Ende zu bringen

gisch ist. Darauf folgt ein klarer Entscheidungsrahmen: Welche Risiken akzeptieren wir, welche nicht? Nur das Management kann den Risikoappetit steuern und entsprechend priorisieren. Ergänzt um Statuskennzahlen und Reviews wird Cybersicherheit Teil der regulären Unternehmenssteuerung. Damit ist der Führungsanspruch klar definiert.

Schmid: Damit NIS-2 nicht als IT-Sache abgetan wird, muss es von Anfang an als Managementaufgabe positioniert werden. Die Unternehmensleitung priorisiert Risiken, legt Zielniveaus fest und trifft Entscheidungen – nicht die technische Umsetzung. Sobald wesentliche Cyber- und Ausfallrisiken regelmäßig auf dieser Ebene adressiert und entschieden werden, wird NIS-2 automatisch Teil der Unternehmenssteuerung. Zugleich braucht es klare Zuständigkeiten: Management für Governance und Entscheidungen, IT und Fachbereiche für die Umsetzung. Managementgerechte Berichte stellen Auswirkungen auf Geschäftsprozesse statt technischer Details in den Vordergrund. NIS-2 sollte in bestehende Führungs- und Entscheidungsroutinen integriert werden, nicht als Sonderprojekt laufen. Gelebt wird es, wenn Führungskräfte entscheiden und Verantwortung übernehmen – nicht, wenn Dokumentation entsteht.

Andreas Grau ist Head of Cybersecurity bei Consileon und mehrfach als Top Cybersecurity Consultant & Leader ausgezeichnet. Seit über 15 Jahren unterstützt er Unternehmen dabei, Cybersecurity, Governance und Risikomanagement pragmatisch und wirkungsorientiert zu gestalten, v. a. in Branchen wie Finanzwirtschaft. Er hat mehr als 50 Projekte erfolgreich geleitet und war u. a. als Interim Manager im Bereich kritischer Finanzinfrastrukturen tätig.

Herr Grau, wie schaffen Sie es, die Geschäftsführung für Cyber-Risiken zu sensibilisieren, ohne Angst zu schüren? Und welche Argumente wirken am besten?

Ich beginne damit zu zeigen, dass Cyberrisiken – wie im klassischen Risikomanagement – nicht nur Bedrohungen sind, sondern Hinweise darauf geben, wo ein Unternehmen widerstandsfähiger werden kann. Dieser Blick auf Auswirkungen und Chancen führt zu einer konstruktiveren Grundhaltung und nimmt dem Thema viel von seiner Schwere. Wichtig ist außerdem, einen Perfektionsanspruch zu vermeiden. Ein nachvollziehbarer, angemessener Weg gibt Sicherheit und macht deutlich, dass Führungskräfte das Thema steuern können, ohne sofort vollständige Lösungen zu haben. Entscheidungen müssen dabei auch bei unvollständigen Informationen möglich bleiben. Eine klar risikobasierte Priorisierung, die Bestandteil der erwähnten Unternehmenssteuerung ist, schafft Orientierung und verhindert, dass Unsicherheit zu Blockaden oder Angst führt.

Viele Mittelständler haben knappe Teams. Wie priorisieren Sie Maßnahmen, damit das Tagesgeschäft nicht leidet – und was lassen Sie bewusst weg?

Schmid: Priorität haben die Maßnahmen, die unmittelbar das größte Risiko reduzieren: Patch-Management, Zugriffsregeln, Backups, ein einfacher Incident-Response-Prozess. Die Pflichtanforderungen werden zunächst minimal funktionsfähig umgesetzt – ohne Perfektionsanspruch. Einfache Prozesse mit etablierten Tools helfen, den Aufwand gering zu halten. Klare Rollenverteilung verhindern Reibungsverluste. Verzichtet wird dagegen auf alles ohne echten Sicherheitsgewinn: Überdokumentation, umfangreiche Policy-Sammlungen, komplexe Risiko Scorings oder „Compliance-Show"-Projekte. NIS-2 ist ein kontinuierlicher Prozess. Wer sich auf die risikoreduzierenden Kernmaßnahmen konzentriert und Schritt für Schritt vorgeht, schützt das Unternehmen, ohne zu überlasten.

Grau: Maßnahmen werden anhand der Folgen priorisiert, die ihre Nichtumsetzung hätte, in Kombination mit der Eintrittswahrscheinlichkeit ebendieser Folgen. Weglassen sollte man alles, was hohen Aufwand erzeugt, aber wenig Nutzen stiftet, etwa überdimensionierte Frameworks oder Dokumentation ohne klaren Zweck. Ein klarer Plan („was jetzt, was später") hält die Organisation handlungsfähig.

Bleiben wir kurz dabei, Herr Grau. Woran erkennt die Geschäftsleitung, ob die NIS-2-Maßnahmen wirken? Welche zwei bis drei Kennzahlen sind wirklich aussagekräftig, ohne sich in Details zu verlieren?

Wirksamkeit zeigt sich daran, dass die priorisierten Themenfelder nachvollziehbar vorankommen. Eine kompakte Statusübersicht macht Fortschritte sichtbar. Zusätzlich ist die Zeitspanne zwischen der Meldung einer Auffälligkeit und ihrer Bearbeitung aussagekräftig – unabhängig davon, ob am Ende ein gravierender Vorfall vorlag. Sinkende Reaktionszeiten zeigen, dass Prozesse greifen und Verantwortlichkeiten funktionieren. Ergänzend können KI-Analysen eine Tendenz erkennen, etwa ob das Sicherheitsniveau steigt oder Risiken zunehmen. Das ersetzt keine formale Bewertung, liefert aber ein schnelles Stimmungsbild für das

Bernhard Schmid arbeitet als Consultant bei der Firma 4IoT GmbH in Freiburg und berät vor allem mittelständische Firmen in den Bereichen IT-Security, IT-Infrastruktur und IT-Betrieb mit einer mehr als 40-jährigen Berufserfahrung.

Management und unterstützt die Einordnung, ob man sich in die richtige Richtung bewegt.

Herr Schmid, „Dritte“ und Lieferanten bleiben oft blinde Flecken. Wie lässt sich die Lieferkettensicherheit praxistauglich steuern – mit zumutbarem Aufwand und klaren Nachweisen?

„Dritte“ und Lieferanten lassen sich praxistauglich steuern, wenn man sie gezielt nach Kritikalität priorisiert. Kritische Lieferanten sind jene, deren Ausfall den Betrieb spürbar beeinträchtigen würde. Nur für sie werden Risiken betrachtet und dokumentiert. Für kritische Lieferanten gelten einfache Mindestanforderungen: Ansprechpartner, Regelungen zur Informationssicherheit, Incident-Meldung und ein kontrolliertes Vertragsende. Der Aufwand bleibt überschaubar, da keine umfassenden Audits nötig sind. Der Nachweis erfolgt schlank und nachvollziehbar durch eine Lieferantenliste mit Kritikalität, einzelne Risikoeinträge im Risikoregister und Vertrags- oder Exit-Regelungen, fokussiert auf tatsächliche Abhängigkeiten.

Wenn Sie einen Blick nach vorn werfen: Was wird sich durch NIS-2 in der Zusammenarbeit zwischen Unternehmen und Wirtschaftsprüfern in den nächsten zwei Jahren am stärksten verändern?

Grau: Die Zusammenarbeit verschiebt sich von der reinen Prüfung hin zur gemeinsamen Steuerung. NIS-2 verlangt nachvollziehbare Entscheidungen, klare Zuständigkeiten und nachweisbare Wirksamkeit; und genau hier wird die Expertise von Wirtschaftsprüfern stärker gefragt sein. Unternehmen werden häufiger mit strukturierten, gut begründeten Nachweisen arbeiten und Auswirkungen auf Betriebsfähigkeit und Lieferketten einordnen müssen. So entsteht eine Rolle, in der Wirtschaftsprüfer Orientierung geben, indem sie Risiken im genauen Unternehmenskontext nachvollziehen.
Schmid: Ich rechne damit, dass sich die Zusammenarbeit mit Prüfern von reiner Dokumentationsprüfung hin zu Wirksamkeits- und Governance-Beurteilung verschiebt. Auch wenn die NIS-2-Umsetzung in Deutschland dem neuen BSI-Gesetz eine Konkretisierung in Richtung Nachweisprüfung mitgegeben hat, gehe ich davon aus, dass Prüfer stärker darauf achten werden, wie Risiken priorisiert, Entscheidungen getroffen und Verantwortlichkeiten wahrgenommen werden, ohne sich in technischen Detailfragen zu verlieren. Unternehmen, die NIS-2 als Management und Steuerungsthema leben, werden Prüfungen dadurch strukturierter, dialogorientierter und effizienter durchlaufen.

„Der wichtigste Rat ist es, NIS-2 konsequent risikobasiert und verhältnismäßig umzusetzen.“