sure[secure]
your security operations center

secure mag

NIS2 OHNE ILLUSIONEN

Was Unternehmen jetzt wirklich entscheiden, aufbauen und betreiben müssen

Executive Summary

NIS2 wird derzeit vor allem als regulatorische Aufgabe behandelt. Leitfäden erklären Anwendungsbereiche, Betroffenheit und Fristen, Checklisten bewerten Reifegrade und Maßnahmen. Was dabei häufig zu kurz kommt, ist eine ehrliche Auseinandersetzung mit der Frage, was NIS2 für die tatsächliche Handlungsfähigkeit von Unternehmen bedeutet.

Dieses Whitepaper richtet sich an Geschäftsführungen, Vorstände und IT-Leitungen, die NIS2 nicht als formale Pflicht, sondern als operative Realität verstehen. Es unterstützt dabei, Prioritäten zu setzen, Entscheidungsfähigkeit herzustellen und begrenzte Ressourcen dort einzusetzen, wo sie im Ernstfall Wirkung entfalten. Der Fokus liegt nicht auf Vollständigkeit oder Maßnahmenlisten, sondern auf der Frage, welche organisatorischen und führungsbezogenen Entscheidungen jetzt notwendig sind, um NIS2 wirksam zu betreiben.

Der zentrale Befund ist einfach, aber unbequem: NIS2 ist kein Dokumentationsproblem. NIS2 ist ein Führungs- und Betriebsproblem.

Unternehmen scheitern selten daran, dass sie Anforderungen nicht kennen. Sie scheitern daran, dass Verantwortung diffus bleibt, Prioritäten nicht entschieden werden, Ressourcen fehlen und Maßnahmen zwar beschrieben, aber nicht betrieben werden. Für Geschäftsführungen, Vorstände und IT-Leitungen stellt sich damit weniger die Frage, ob gehandelt werden muss, sondern:

- wo zuerst investiert werden sollte,
- welche Maßnahmen tatsächlich Wirkung entfalten,
- und welche Anforderungen bewusst priorisiert oder gestaffelt werden müssen.

Dieses Whitepaper liefert dafür einen Entscheidungsrahmen.

Warum fast alle NIS2-Leitfäden am Ziel vorbeigehen

Der Markt für NIS2-Leitfäden ist in kurzer Zeit stark gewachsen. Inhaltlich ähneln sich viele Veröffentlichungen auffallend. Sie erklären die Richtlinie, ordnen Betroffenheit ein und leiten daraus Maßnahmenkataloge, Reifegradmodelle oder Checklisten ab. Formal ist dieser Ansatz korrekt. Praktisch bleibt er häufig wirkungslos.

Der zentrale Denkfehler liegt in der Annahme, dass regulatorische Konformität automatisch zu operativer Handlungsfähigkeit führt. In der Realität zeigt sich jedoch oft ein anderes Bild. Zwar verfügen Unternehmen über Richtlinien, benannte Verantwortlichkeiten und dokumentierte Maßnahmen, im Ernstfall sind sie jedoch schlecht koordiniert, zögerlich in der Entscheidungsfindung und unsicher in der Kommunikation. Verantwortung verschwimmt genau in dem Moment, in dem Klarheit erforderlich wäre.

NIS2 verschärft diesen Widerspruch. Die Richtlinie verlangt nicht nur Prävention, sondern explizit Fähigkeiten zur Erkennung, Reaktion und Wiederherstellung. Diese Fähigkeiten lassen sich nicht „abarbeiten“. Sie müssen betrieben, eingeübt und aktiv geführt werden.

Hinzu kommt, dass viele Leitfäden implizit von homogenen Reifegraden ausgehen. Große Organisationen sind jedoch geprägt von historisch gewachsenen IT-Landschaften, knappen Ressourcen, komplexen Lieferketten und fragmentierten Zuständigkeiten. In diesem Umfeld erzeugen umfangreiche Maßnahmenkataloge vor allem Aktionismus, aber keine Priorisierung.

Was fehlt, ist ein Rahmen, der beantwortet, welche Entscheidungen jetzt getroffen werden müssen, welche Maßnahmen kurzfristig Wirkung entfalten und wo bewusstes Weglassen sinnvoller ist als formale Vollständigkeit.

NIS2 als Entscheidungsrahmen

Eine wirksame Umsetzung von NIS2 erfordert einen Perspektivwechsel. Die Richtlinie ist kein Projekt mit klar definiertem Ende, sondern beschreibt einen dauerhaften Betriebszustand. Dieser Zustand betrifft Führung, Organisation und Technik gleichermaßen.

Auf der Führungsebene geht es um Grundsatzentscheidungen. Dazu zählen die bewusste Akzeptanz oder Ablehnung von Risiken, die Priorisierung kritischer Geschäftsprozesse und die Bereitstellung von Ressourcen. Diese Entscheidungen sind nicht delegierbar. Sie liegen bei Geschäftsführung und Vorstand.

Auf organisatorischer Ebene entscheidet sich, ob diese Führungsentscheidungen Wirkung entfalten. Rollen, Eskalationswege, Entscheidungsbefugnisse und Kommunikationsstrukturen müssen klar geregelt und akzeptiert sein. Ohne diese Klarheit bleiben technische Maßnahmen isoliert und wirkungslos.

Erst auf der technischen Ebene geht es um konkrete Fähigkeiten zur Erkennung, Reaktion und Wiederherstellung. Technik ist notwendig, aber nicht hinreichend. Sie entfaltet ihren Wert nur, wenn sie in funktionierende Abläufe eingebettet ist.

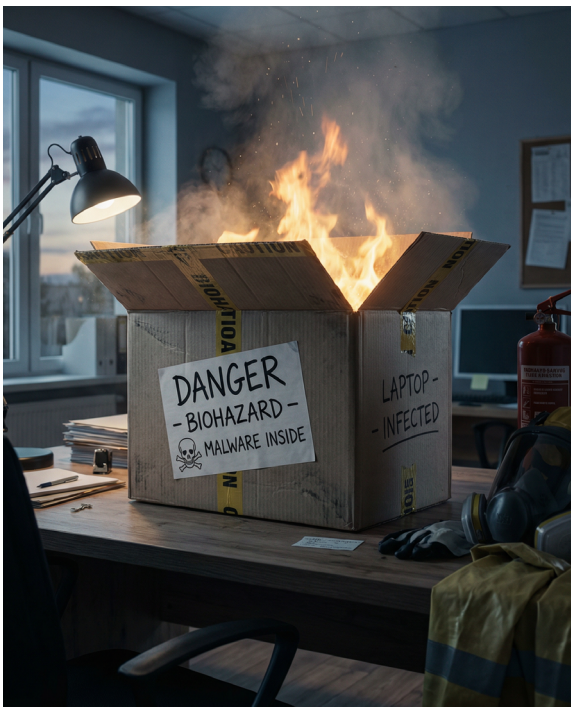
Viele NIS2-Initiativen scheitern, weil diese Ebenen vermischt oder in falscher Reihenfolge adressiert werden. Technik wird eingeführt, bevor Verantwortung geklärt ist. Prozesse werden dokumentiert, ohne dass Entscheidungen vorbereitet sind. NIS2 zwingt Unternehmen jedoch implizit dazu, diese Reihenfolge einzuhalten, und zwar unabhängig davon, wie der Gesetzestext interpretiert wird.

Warum Wirkung verloren geht

NIS2-Initiativen verlieren häufig nicht am Anfang, sondern im Betrieb an Wirkung. Entscheidungen werden nicht nachgeschärft, Maßnahmen nicht weiterentwickelt und Verantwortung nicht aktiv wahrgenommen. Wirksamkeit entsteht nicht durch den Start, sondern durch kontinuierliche Steuerung.

Der Ernstfall als Ausgangspunkt

NIS2 wird häufig aus der Perspektive der Prävention gedacht. Entscheidend ist jedoch nicht, ob ein Vorfall eintritt, sondern wie ein Unternehmen damit umgeht, wenn er eintritt. Die folgenden Szenarien sind keine Ausnahmen, sondern typische Situationen in großen Organisationen.



Ransomware legt zentrale Systeme lahm

Nachts werden mehrere Systeme verschlüsselt. Am Morgen sind zentrale Anwendungen nicht verfügbar, Geschäftsprozesse stehen still. Die IT erkennt schnell den Ernst der Lage und beginnt mit der Analyse. Gleichzeitig zeigt sich, dass grundlegende Entscheidungen ausbleiben.

Typisch ist eine Situation, in der

- die technische Analyse läuft, aber keine Gesamtkoordination stattfindet,
- unklar ist, wer den Vorfall offiziell als erheblich einstuft,
- Unsicherheit darüber besteht, wann und wie das Management informiert werden muss.

Die Organisation arbeitet, aber sie wird nicht geführt. Aus Sicht von NIS2 ist weniger relevant, wie der Angriff technisch erfolgte. Entscheidend ist, ob das Unternehmen in der Lage ist, unter Zeitdruck Entscheidungen zu treffen, zu kommunizieren und zu handeln, auch wenn die Informationen unvollständig sind.

Ein Dienstleister wird zum Risiko

Ein externer Dienstleister meldet einen Sicherheitsvorfall oder fällt kurzfristig aus. Noch ist unklar, ob eigene Systeme betroffen sind. Gleichzeitig sind kritische Leistungen eingeschränkt oder nicht verfügbar.

In vielen Unternehmen zeigt sich dann, dass

- Abhängigkeiten zwar dokumentiert, aber nicht priorisiert sind,
- Sicherheitsbewertungen existieren, aber keine operative Handlungsfähigkeit liefern,
- Zuständigkeiten für Eskalation und Nachverfolgung unklar bleiben.

NIS2 verlangt hier mehr als formale Bewertung. Wer Risiken kennt, muss sie aktiv managen. Dokumentierte Erkenntnisse erzeugen Verantwortung und damit Entscheidungsdruck.

Insider oder Fehlkonfiguration bleiben unbemerkt

Nicht jeder Vorfall beginnt mit einem Alarm. Fehlkonfigurationen, übermäßige Berechtigungen oder interne Auffälligkeiten entwickeln sich schleichend. Hinweise werden wahrgenommen, aber nicht eskaliert. Protokolle existieren, werden jedoch nicht ausgewertet.

Das Problem ist selten rein technischer Natur. Es liegt in

- fehlender Eskalationskultur,
- unklaren Zuständigkeiten und
- der Unsicherheit, wann ein Signal relevant genug ist, um gehandelt zu werden.

NIS2 adressiert genau diese Grauzone. Gefordert ist nicht die lückenlose Vermeidung solcher Situationen, sondern die Fähigkeit, relevante Hinweise systematisch zu bewerten und daraus rechtzeitig Handlungen abzuleiten. Entscheidend ist, ob Organisationen klare Kriterien, Verantwortlichkeiten und Prozesse etabliert haben, um auch schleichende Risiken wirksam zu steuern.

PODCAST

CYBER SECURITY Basement

In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking". Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.

Jetzt reinhören

Spotify

Apple Podcast

YouTube Music

amazon music

und noch mehr...

Incident Response und Meldepflichten

Meldepflichten werden häufig als formale Fristen interpretiert. In der Praxis sind Sicherheitsvorfälle jedoch von Unsicherheit geprägt. Innerhalb der ersten 24 Stunden liegen in der Regel weder belastbare Ursachenanalysen noch vollständige Schadensbilder vor. Das ist kein Versäumnis, sondern Realität.

NIS2 verlangt keine perfekte Erstmeldung, sondern nachvollziehbares Handeln. Entscheidend ist, dass ein Unternehmen zeigen kann, dass

- ein Vorfall erkannt wurde,
- angemessen reagiert wird,
- und die Situation aktiv gemanagt wird.

„Wir wissen es noch nicht“ ist dabei zulässig, sofern diese Aussage Teil eines strukturierten Prozesses ist.

Meldepflichten sind kein einmaliger Akt, sondern ein fortlaufender Ablauf aus Erstmeldung, Zwischenberichten und Abschlussmeldung. Ohne Übung bleiben diese Prozesse theoretisch. Erst im Ernstfall zeigt sich, ob Eskalation akzeptiert ist, Entscheidungen getroffen werden und Führung funktioniert.

Früherkennungssysteme

Früherkennung wird häufig auf technische Systeme reduziert. In der Praxis entsteht sie aus dem Zusammenspiel organisatorischer Klarheit, funktionierender Prozesse und technischer Signale. Fehlt eine dieser Ebenen, verliert das Gesamtsystem an Wirksamkeit.

Viele Hinweise auf Vorfälle entstehen lange vor einem technischen Alarm. Ungewöhnliche Beobachtungen, Rückfragen von Dienstleistern oder Unsicherheiten im Betrieb bleiben folgenlos, wenn Eskalation nicht gewollt ist. Früherkennung ist daher auch eine Führungsfrage. Zweifel müssen erlaubt sein, Eskalation darf kein Risiko für den Melder darstellen.

Technische Systeme liefern wertvolle Signale. Ihr Nutzen entsteht jedoch erst, wenn klar ist, wie diese Informationen bewertet, weitergegeben und in Entscheidungen übersetzt werden. Entscheidend ist, ob Führung Eskalation ausdrücklich ermöglicht und Verantwortung für Entscheidungen auch dann übernimmt, wenn Informationen unvollständig sind. NIS2 verlangt keine lückenlose Überwachung, sondern die Fähigkeit, erhebliche Vorfälle rechtzeitig zu erkennen und einzuordnen.

Die Perspektive im Ernstfall

Im Ernstfall zählt, ob ein Vorfall erkennbar geführt wird. Bewertet werden Entscheidungsfähigkeit, Nachvollziehbarkeit und aktive Steuerung über Zeit. Unsicherheit ist akzeptiert, fehlende Führung nicht.

Lieferkette und Dienstleister

Lieferkettenmanagement ist eines der formell am besten abgedeckten Themen, aber eines der operativ schwächsten. Bewertungen sind häufig veraltet, kritische Abhängigkeiten nicht priorisiert und identifizierte Mängel bleiben folgenlos.

Das eigentliche Risiko entsteht nicht durch fehlende Dokumentation, sondern durch fehlendes Handeln. Wenn Missstände erkannt werden, müssen Maßnahmen eingefordert, umgesetzt und überprüft werden. Genau hier fehlen in vielen Organisationen Ressourcen und klare Zuständigkeiten.

NIS2 verschärft diesen Punkt. Bekannte, aber nicht adressierte Risiken lassen sich im Ernstfall kaum rechtfertigen. Eine Konsequenz ist die Notwendigkeit zur Priorisierung. Nicht alle Dienstleister sind gleich kritisch. Weniger, aber gezielter gemanagte Beziehungen erhöhen die tatsächliche Resilienz.

Management-Verantwortung

NIS2 adressiert die Verantwortung der Unternehmensleitung klar. Entscheidend ist jedoch nicht die Angst vor persönlicher Haftung, sondern die aktive Wahrnehmung von Steuerung.

Bestimmte Entscheidungen sind nicht delegierbar. Dazu gehören

- die Festlegung von Prioritäten,
- die bewusste Akzeptanz von Restrisiken,
- die Bereitstellung von Ressourcen,
- und die Einordnung erheblicher Vorfälle.

Dokumentierte Entscheidungen sind dabei kein Selbstzweck, sondern Schutz. Regelmäßige Lageberichte, klare Beschlusslagen und transparente Risikoentscheidungen zeigen, dass Verantwortung aktiv wahrgenommen wird, ohne dass es zu einer operativen Einmischung in technische Details kommt.

Budget, Priorisierung und Realität

Die Annahme, NIS2 lasse sich nebenbei umsetzen, ist einer der häufigsten Gründe für das Scheitern von Initiativen. Die geforderten Fähigkeiten müssen dauerhaft betrieben werden. Ohne zusätzliche Ressourcen entstehen formale Erfüllung, operative Überlastung und wachsende Abhängigkeiten von externen Dienstleistern.

Budget ist Ausdruck von Priorisierung. Ohne klare finanzielle und personelle Entscheidungen bleibt NIS2 fragmentiert. Gleichzeitig ist Overengineering ein reales Risiko. Wirksam ist nicht, was maximal dokumentiert ist, sondern was im Ernstfall funktioniert.

Der Weg in den wirksamen Betrieb

„Aus meiner Erfahrung beginnt wirksame Sicherheit immer mit Führung. Verantwortlichkeiten, Entscheidungswege und Eskalationskriterien müssen klar und verbindlich geregelt sein, denn erst auf dieser Grundlage können operative Maßnahmen ihre Wirkung entfalten. Gleichzeitig geht es in der Praxis nicht darum, alles auf einmal umzusetzen. Handlungsfähigkeit entsteht durch einen klar abgegrenzten Zeitraum mit konkreten Zielen. Entscheidend ist, dass daraus ein stabiler Betrieb entsteht und keine kurzfristige Initiative."

Erik Krüger, Information Security Officer & GRC Consultant

Fazit

NIS2 ist kein Projekt, sondern ein Führungsrahmen. Wer die Richtlinie als Pflichtübung versteht, wird formale Anforderungen erfüllen, aber im Ernstfall scheitern. Wer sie als Anlass nutzt, Verantwortung zu klären, Prioritäten zu setzen und operative Fähigkeiten aufzubauen, gewinnt echte Resilienz.

Vertiefung:

Diese Podcastfolge zu ISMS und NIS2 beleuchtet Informationssicherheit als langfristigen Organisations- und Führungsprozess und ordnet zentrale Anforderungen aus der Umsetzungsperspektive ein.

Weitere Informationen zum Thema:

Podcast-Folge:

NIS2-Richtlinie als klarer Weckruf:
Auf dem Weg zu echter Cyberresilienz

Podcast-Folge:

ISMS und NIS 2 auf der Zielgeraden:
Ausdauersport der Informationssicherheit

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de