NIS2

ASSESSMENT

Eine kompakte Einordnung für
Geschäftsführung und IT-Leitung

securance

MANAGEMENT SUMMARY

NIS2 ist keine technische Richtlinie, sondern eine Reaktion auf ein strukturelles Risiko. Cybervorfälle wirken heute nicht mehr isoliert, sondern entlang von Lieferketten und Abhängigkeiten. Sie beeinträchtigen Produktionsfähigkeit, Dienstleistungsfähigkeit und im Einzelfall die Stabilität ganzer Geschäftsmodelle.

Gleichzeitig werden Risiken in vielen Unternehmen operativ adressiert, aber nicht konsistent gesteuert. NIS2 setzt genau hier an. Die Richtlinie verlagert Cybersicherheit in die Verantwortung der Unternehmensleitung und fordert eine nachvollziehbare, dokumentierte und dauerhaft überwachbare Risikosteuerung.

Für betroffene Unternehmen bedeutet das einen klaren Perspektivwechsel: Nicht die Existenz einzelner Maßnahmen ist entscheidend, sondern ob diese Maßnahmen Teil eines konsistenten, steuerbaren Systems sind.

Das NIS2 Assessment macht diese Steuerbarkeit sichtbar und schafft eine belastbare Grundlage für fundierte Entscheidungen auf Management-Ebene.

MYTHEN UND REALITÄT

Mythos:
„NIS2 betrifft vor allem KRITIS."

Realität:
Die Regulierung betrifft weite Teile des Mittelstands. Entscheidend ist die Rolle in kritischen Wertschöpfungsketten, nicht die klassische KRITIS-Zuordnung.

Mythos:
„Technische Sicherheit reicht aus."

Realität:
Bewertet wird nicht die Anzahl der Maßnahmen, sondern die Nachvollziehbarkeit von Risikoentscheidungen. Ohne Dokumentation gilt Sicherheit als nicht steuerbar.

Mythos:
„Wir müssen erst alles vollständig umsetzen."

Realität:
Regulatorisch entscheidend ist Priorisierung. Maßnahmen müssen in eine konsistente Steuerungslogik eingebettet sein, nicht vollständig umgesetzt werden.

AUSGANGSPUNKT:

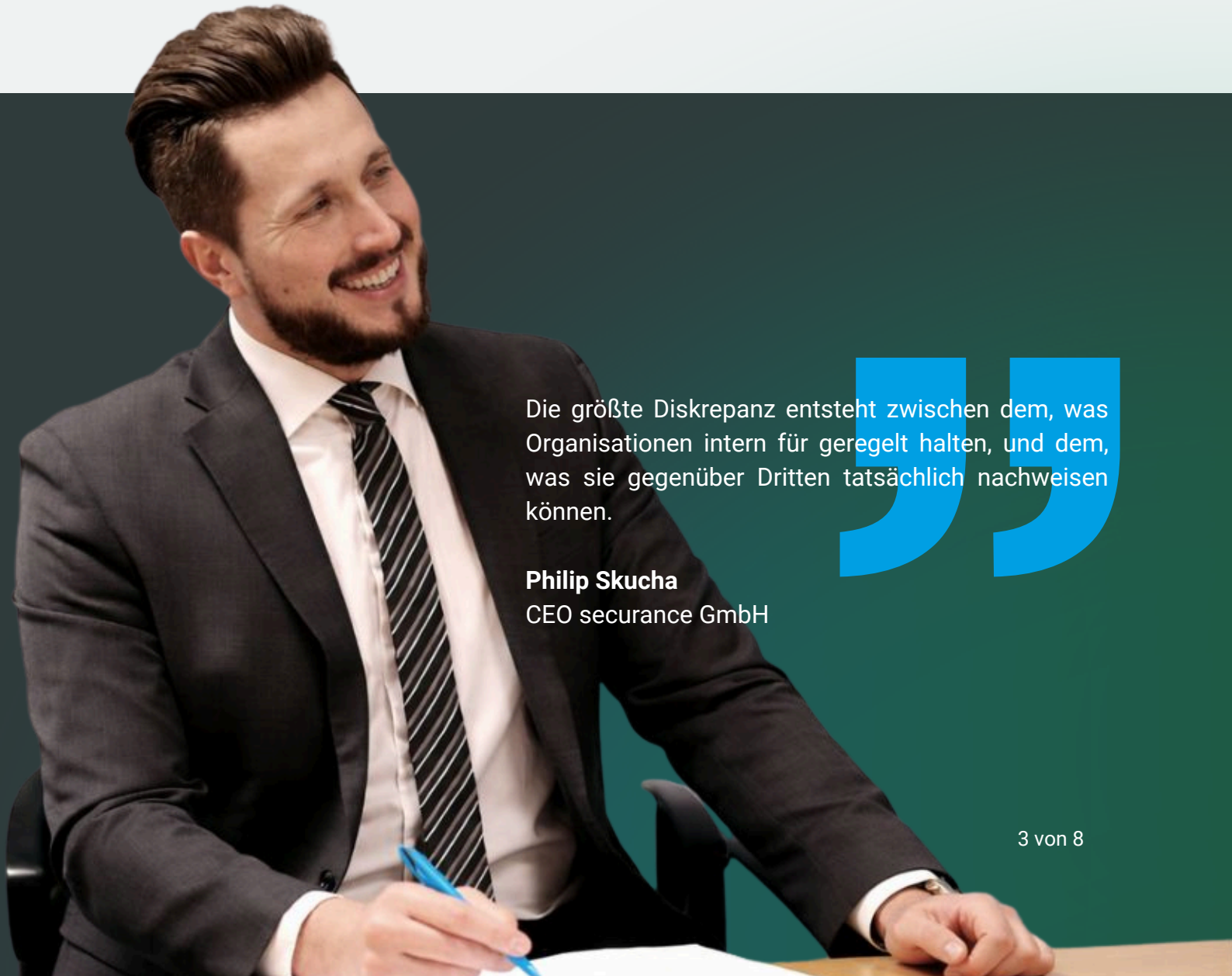
WO STEHT DAS UNTERNEHMEN WIRKLICH?

Die Umsetzung von NIS2 scheitert selten an fehlenden Maßnahmen, sondern an einer unklaren Ausgangsbasis. Viele Unternehmen wissen, dass sie betroffen sind, können jedoch nicht belastbar abgrenzen, wo die Regulierung tatsächlich greift.

In der Praxis entstehen dadurch zwei typische Fehlentwicklungen:

- Maßnahmen werden zu breit angesetzt und verlieren an Fokus
- oder sie greifen zu kurz und lassen regulatorische Lücken bestehen.

Gerade in gewachsenen Strukturen fehlt häufig eine klare Zuordnung von Risiken, Prozessen und Verantwortlichkeiten.



> Die größte Diskrepanz entsteht zwischen dem, was Organisationen intern für geregelt halten, und dem, was sie gegenüber Dritten tatsächlich nachweisen können.

Philip Skucha
CEO securance GmbH

ZENTRALE KLÄRUNGSFRAGEN

- Welche Geschäftsprozesse sind regulatorisch relevant?
- Welche organisatorischen Einheiten fallen konkret unter NIS2?
- Wie wird die Sicherheit der Lieferkette und kritischer Dienstleister gewährleistet?
- Wie stellt die Geschäftsführung Compliance und Haftungsfreistellung sicher?

KERNFAKTEN FÜR DIE GESCHÄFTSFÜHRUNG

29.000

BETROFFENE UNTERNEHMEN

Die Regulierung betrifft erstmals große Teile des industriellen und digitalen Mittelstands.

10 Mio €

ODER 2 % UMSATZ

Neben Unternehmensstrafen entsteht persönliche Haftung auf Leitungsebene.

24 / 72

STUNDEN MELDEFRISTEN

Vorfallsmeldungen erfordern belastbare Entscheidungs- und Eskalationsprozesse.

Verantwortung

DER GESCHÄFTSFÜHRUNG

Cybersicherheit wird zur nicht delegierbaren Leitungsaufgabe.

WARUM IN EIN NIS2 ASSESSMENT INVESTIEREN

Viele Unternehmen verfügen über funktionierende Sicherheitsmaßnahmen. Die eigentliche Schwäche liegt jedoch selten in der Umsetzung einzelner Kontrollen, sondern in der fehlenden Verknüpfung zu einer konsistenten Steuerungslogik.

Was intern als ausreichend wahrgenommen wird, ist häufig historisch gewachsen. Entscheidungen wurden situativ getroffen, ohne durchgängige Bewertungslogik oder konsistente Dokumentation. Gerade intern als „funktionierend“ bewertete Strukturen erweisen sich in der Prüfung häufig als nicht belastbar.

Genau hier liegt die Herausforderung: Nicht die Maßnahmen selbst, sondern deren Einordnung, Steuerbarkeit und Nachweisfähigkeit sind entscheidend. Ein NIS2 Assessment geht deshalb über eine Bestandsaufnahme hinaus.

Es analysiert,

- wie Risiken tatsächlich bewertet werden,
- wie Entscheidungen zustande kommen, und
- ob bestehende Maßnahmen Teil eines konsistenten Steuerungsmodells sind.

Der Mehrwert liegt in der Tiefe der Analyse. Bewertet wird nicht nur, ob Kontrollen vorhanden sind, sondern ob sie organisatorisch verankert, nachvollziehbar dokumentiert und dauerhaft steuerbar sind.

Für die Geschäftsführung entsteht dadurch eine belastbare Grundlage zur Priorisierung und Risikosteuerung.

Erst durch eine externe Bewertung wird sichtbar, wo Annahmen und tatsächliche Risiken auseinanderlaufen. Was intern als ausreichend gilt, hält einer strukturierten Prüfung häufig nicht stand.

Sidney Bauer
Cyber Specialst, securance GmbH

STRUKTURIERTE NIS2-READINESS

INNERHALB KLAR DEFINIERTER ZEITRÄUME

Die Umsetzung von NIS2 ist kein rein technisches Projekt, sondern eine organisatorische Strukturaufgabe. Unternehmen erzielen dann schnell Fortschritte, wenn sie entlang klar definierter Schritte vorgehen und Maßnahmen in ein konsistentes Steuerungsmodell überführen.

Regulierung ersetzt keine Sicherheit, definiert jedoch einen klaren, überprüfbaren Maßstab. NIS2 transformiert Cybersicherheit von einer technischen Disziplin zu einer Organisationspflicht auf Leitungsebene.

Die Erfahrung aus der Praxis zeigt: Der Weg zur strukturierten NIS2-Readiness ist in vielen Fällen deutlich kürzer als erwartet. Ein Großteil der Unternehmen erreicht innerhalb weniger Monate eine belastbare Ausgangsbasis, vorausgesetzt, der Fokus liegt auf Einordnung, Priorisierung und klaren Verantwortlichkeiten statt auf isolierten Einzelmaßnahmen.

Entscheidend ist dabei nicht die Geschwindigkeit einzelner Umsetzungen, sondern die Konsistenz der zugrunde liegenden Struktur.

MANAGEMENT TAKE-AWAYS

- Die zentrale Herausforderung liegt in der fehlenden Steuerungsstruktur
- Nicht dokumentierte Entscheidungen gelten regulatorisch als nicht getroffen
- Gewachsene Sicherheitslandschaften sind selten konsistent steuerbar
- Lieferkettenrisiken bleiben in der Verantwortung des Unternehmens
- Priorisierung erfordert eine klare Risikologik

SCHLUSSWORT

NIS2 verändert nicht die Sicherheitsrealität, sondern den Maßstab ihrer Bewertung. Unternehmen stehen vor der Aufgabe, Sicherheit nicht nur umzusetzen, sondern als steuerbaren, nachvollziehbaren Prozess zu etablieren.

Organisationen, die diese Perspektive frühzeitig einnehmen, schaffen nicht nur regulatorische Sicherheit, sondern eine belastbare Grundlage für unternehmerische Entscheidungen.

EINORDNUNG STARTEN

Jetzt strukturiert Reifegrad bestimmen

securance GmbH
Dreischeibenhaus 1
40211 Düsseldorf

+49 (0)211 882 302 83
kontakt@securance.de