VANTARION

# Lieferkettensicherheit

## So erfüllen KMU Anforderungen von Kunden, NIS2 & ISO gleichzeitig

Ein Praxisleitfaden für
Geschäftsführung, Einkauf, QM & ISB

# MANAGEMENT SUMMARY

## Cybersicherheit endet nicht am eigenen Werkstor.

Lieferkettensicherheit ist längst kein isoliertes IT-Thema mehr. Sie ist ein strategisches Managementthema.

Ob Industrie, Pharma, Gesundheitswesen oder technologiegetriebene Dienstleistungsbranchen – regulatorische Anforderungen und kundenseitige Vorgaben machen deutlich: Unternehmen tragen Verantwortung nicht nur für die eigene Informationssicherheit, sondern auch für die Sicherheit ihrer Partner und Dienstleister.

ISO 27001 fordert eine risikobasierte Steuerung externer Parteien.
TISAX verlangt nachvollziehbare Lieferantenkontrollen.
NIS2 verpflichtet ausdrücklich zur Berücksichtigung von Risiken entlang der Lieferkette.

Gleichzeitig steigt der wirtschaftliche Druck: Kunden erwarten belastbare Nachweise, Versicherer prüfen Risikostrukturen, und Sicherheitsvorfälle bei Dienstleistern wirken sich unmittelbar auf das eigene Unternehmen aus.

Die Herausforderung besteht nicht darin, möglichst viele Lieferanten zu kontrollieren. Die Herausforderung besteht darin, Lieferanten strukturiert in das eigene Risikomanagement zu integrieren.

Ein professioneller Ansatz basiert auf einer klaren Logik:

- ☑ **Welche Geschäftsprozesse sind von externen Partnern abhängig?**
- ☑ **Welche Informationswerte oder Systeme werden berührt?**
- ☑ **Welche Bedrohungsszenarien entstehen daraus?**
- ☑ **Welche Maßnahmen sind angemessen?**

Diese systematische Betrachtung, angelehnt an etablierte Methoden wie ISO 27005, schafft eine belastbare Grundlage für Entscheidungen. Sie ermöglicht Verhältnismäßigkeit, Skalierbarkeit und Auditfähigkeit.

Lieferkettensicherheit wird damit nicht zu einem administrativen Zusatzaufwand, sondern zu einem steuerbaren Bestandteil des unternehmensweiten Governance- und Risikorahmens.

Unternehmen, die ihre Lieferantenbeziehungen methodisch bewerten, klare Anforderungen definieren und diese dokumentiert überwachen, schaffen Transparenz – gegenüber Kunden, Aufsichtsbehörden und der eigenen Geschäftsführung.



Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

## LIEFERKETTE ALS TEIL DER RISIKOLOGIK

Lieferanten sind keine isolierten Objekte. Sie sind Bestandteil von:

- ☑ **Geschäftsprozessen**
- ☑ **Informationswerten**
- ☑ **Systemlandschaften**
- ☑ **regulatorischen Verpflichtungen**

Eine belastbare Supplier-Security beginnt daher nicht mit einer Checkliste, sondern mit einer strukturierten Betrachtung:

1. **Prozess: Welche Geschäftsprozesse sind betroffen?**
2. **Asset: Welche Informationen oder Systeme werden berührt?**
3. **Szenario: Welche Bedrohung ergibt sich aus der Lieferantenbeziehung?**
4. **Maßnahme: Welche organisatorischen oder technischen Kontrollen sind erforderlich?**

Diese Logik entspricht der etablierten Risikomethodik nach ISO 27005 und ist anschlussfähig an ISO 27001, TISAX und NIS2.

Tobias Frank,
Gründer und CEO

Als **Head of IT und Verantwortlicher für Informationssicherheit** in Handelsunternehmen und Fertigungsindustrie und habe ich in allen Facetten erlebt, wie aufwändig Informationssicherheit für CxO und Teams im Alltag ist. 20 Jahre lang.

Aus diesem persönlichen Antrieb heraus entwickelten wir VantarIS und gründeten Vantarion.

VantarIS nimmt die Bürokratie aus Normen wie NIS2 und bringt kompetente Sicherheit.

VANTARIS



Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

# VON DER RISIKOANALYSE ZUR TIER-STRUKTUR

Die Einteilung in Supplier-Tiers ist kein Ersatz für eine Risikoanalyse, sondern deren operationalisiertes Ergebnis.

Aus der Bewertung von:

- ☑ Kritikalität des Prozesses
- ☑ Sensitivität der betroffenen Assets
- ☑ Eintrittswahrscheinlichkeit eines Szenarios
- ☑ Auswirkung bei Störung oder Kompromittierung

ergibt sich die Einstufung des Lieferanten in eine Risikokategorie.

### Beispielhafte Ableitung:

#### Kritischer Lieferant

- ☑ Zugriff auf sensible oder regulierte Daten
- ☑ IT-Administrationsrechte
- ☑ Betrieb geschäftskritischer Prozesse
- ☑ Hohe regulatorische Abhängigkeit

#### Hohe Relevanz

- ☑ Unterstützende Prozesse
- ☑ Eingeschränkter Datenzugriff
- ☑ Teilweise Systemintegration

#### Normale Relevanz

- ☑ Keine sicherheitsrelevanten Assets
- ☑ Geringe System- oder Datenabhängigkeit
- ☑ Damit bleibt die Tier-Struktur konsistent mit der Gesamt-Risikologik des Unternehmens.



Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

## VERTRAGLICHE ABSICHERUNG ALS RISIKOMASSNAHME

Im ISO 27005 Kontext sind Vertragsklauseln keine Formalität, sondern Risikobehandlungsmaßnahmen.

Typische sind:

- ☑ Verpflichtung zur Einhaltung definierter Sicherheitsstandards
- ☑ Meldepflicht bei Sicherheitsvorfällen
- ☑ Verpflichtung zur Weitergabe von Anforderungen an Subunternehmer
- ☑ Nachweispflicht zu technischen und organisatorischen Maßnahmen
- ☑ Audit- oder Prüfungsrechte

Die Intensität der vertraglichen Anforderungen ergibt sich aus dem Risikoniveau – nicht aus pauschaler Vorgabe.

## KONTROLLPUNKTE IM RISIKO-LEBENSZYKLUS

Lieferantenrisiken verändern sich im Zeitverlauf. Daher müssen Kontrollpunkte in den Risikomanagementprozess integriert werden:

### 1. Onboarding

- ☑ Risikoanalyse der Lieferantenbeziehung
- ☑ Zuordnung zu Prozess und Asset
- ☑ Dokumentierte Risikobehandlung
- ☑ Vertragsgestaltung als Maßnahme

### 2. Regelmäßige Neubewertung

- ☑ Überprüfung bei Prozessänderungen
- ☑ Anpassung der Schutzanforderungen
- ☑ Aktualisierung von Nachweisen



Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

### 3. Ereignisbasierte Neubewertung

- ☑ Sicherheitsvorfall
- ☑ Änderung regulatorischer Anforderungen
- ☑ Strukturänderungen beim Lieferanten

Lieferkettensicherheit wird so Teil des kontinuierlichen Verbesserungsprozesses, nicht isoliertes Einmalprojekt.

## TYPISCHE SCHWACHSTELLEN

Unternehmen, die Lieferkettensicherheit isoliert behandeln, zeigen häufig:

- ☑ Keine Verknüpfung zur Risikoanalyse
- ☑ Keine Asset-basierte Betrachtung
- ☑ Lieferantenklassifizierung ohne dokumentierte Begründung
- ☑ Maßnahmen ohne zentrale Steuerung
- ☑ Keine Integration ins Management-Reporting

Die Folge: Intransparenz gegenüber Auditoren und Geschäftsführung.

## KONKRETE UMSETZUNGSBAUSTEINE

Lieferkettensicherheit wird wirksam, wenn sie strukturiert dokumentiert und gesteuert wird. Die folgenden Bausteine unterstützen dabei:

### Template: Supplier-Security-Anforderungen

- ☑ Bezug zu betroffenen Prozessen
- ☑ Bezug zu betroffenen Assets
- ☑ Sicherheitsmaßnahmen je Risikoniveau
- ☑ Incident-Meldepflicht



Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

## Template: Mindestanforderungen als Vertragsanlage

- ☑ Verbindliche Sicherheitsanforderungen
- ☑ Bezug zu Schutzbedarfsstufen
- ☑ Regelungen zur Subunternehmersteuerung
- ☑ Audit- und Nachweispflichten

## Checkliste: Supplier-Onboarding in 10 Schritten

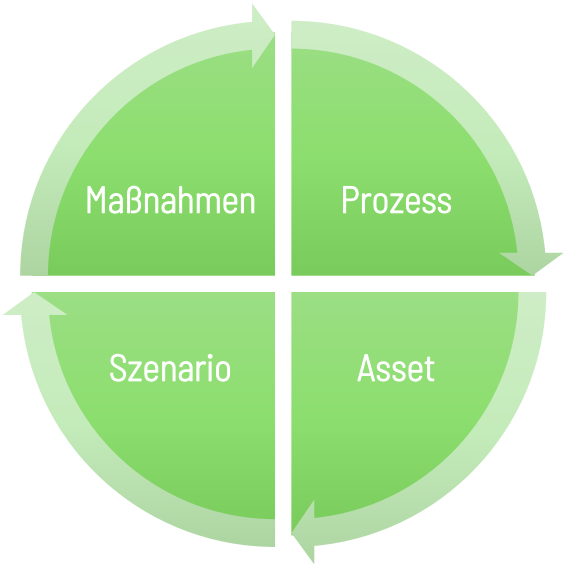
- ☑ Prozessidentifikation
- ☑ Asset-Zuordnung
- ☑ Szenarienbewertung
- ☑ Risikokategorie
- ☑ Maßnahmenfestlegung
- ☑ Vertragsintegration
- ☑ Dokumentation
- ☑ Review-Terminierung
- ☑ Verantwortlichkeitszuweisung
- ☑ Reporting an Management

# FAZIT

Lieferkettensicherheit ist keine isolierte Compliance-Disziplin. Sie ist integraler Bestandteil moderner Unternehmensführung.

Die Frage ist nicht, ob externe Partner Risiken darstellen. Die Frage ist, ob diese Risiken systematisch erkannt, bewertet und gesteuert werden.

Ein strukturierter Ansatz – basierend auf der Logik




ermöglicht es, Lieferantenrisiken nachvollziehbar zu klassifizieren und angemessene Schutzmaßnahmen abzuleiten. Dadurch entsteht keine Überregulierung, sondern kontrollierte Verhältnismäßigkeit.

Unternehmen, die Lieferantenbeziehungen klar dokumentieren, vertraglich absichern und regelmäßig überprüfen, erfüllen nicht nur regulatorische Anforderungen. Sie stärken ihre Resilienz und reduzieren operative Abhängigkeiten. Entscheidend ist dabei nicht die Anzahl der ausgefüllten Fragebögen oder Vertragsklauseln. Entscheidend ist die Integration in das bestehende Risikomanagement und die kontinuierliche Steuerung durch definierte Verantwortlichkeiten und Kontrollpunkte.

Wird die Lieferkette als Bestandteil des Governance-Systems verstanden, entsteht ein konsistenter, auditfähiger und skalierbarer Sicherheitsrahmen.

Lieferkettensicherheit wird damit von einer reaktiven Pflicht zu einem strategischen Steuerungsinstrument.

## Der nächste logische Schritt ist klar:

Lieferantenrisiken systematisch erfassen, strukturiert bewerten und zentral steuern.

- ☑ **Wo diese Transparenz fehlt, entsteht Unsicherheit.**
- ☑ **Wo sie vorhanden ist, entsteht Kontrolle.**



Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de