VANTARION

Haftung & Verantwortung

Was Geschäftsführer bei NIS2, ISO & TISAX wirklich entscheiden müssen

Ein Leitfaden für
Geschäftsführung und Board

MANAGEMENT SUMMARY

Informationssicherheit ist keine delegierbare IT-Aufgabe. Sie ist Führungsverantwortung.

Mit NIS2, ISO 27001 und TISAX wird die Rolle der Geschäftsleitung haftungsrechtlich konkretisiert. Denn nun sind Geschäftsführung und Vorstand verpflichtet, angemessene Risikomanagementmaßnahmen zu beschließen, zu überwachen und deren Wirksamkeit sicherzustellen.

Die zentrale Frage lautet daher nicht:
„Haben wir einen IT-Dienstleister?"

Sondern:
„Haben wir ein steuerbares, dokumentiertes und nachvollziehbares Sicherheitsmanagement?"

Im Ernstfall durch Cyberangriff, Datenschutzvorfall oder Betriebsunterbrechung entscheiden nicht die Existenz technischer Maßnahmen, sondern die Nachweisbarkeit von Governance über die Haftung:

- ☑ **Wurden Risiken bewertet?**
- ☑ **Wurden Entscheidungen dokumentiert?**
- ☑ **Wurden Maßnahmen priorisiert?**
- ☑ **Wurde regelmäßig berichtet?**
- ☑ **Hat das Management aktiv gesteuert?**

Dieses Whitepaper zeigt, welche Entscheidungen nicht delegierbar sind, welche Nachweise im Haftungsfall schützen und wie ein wirksames Reporting für Geschäftsführung und Board strukturiert sein sollte.

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

INFORMATIONSSICHERHEIT ALS FÜHRUNGSAUFGABE

Mit NIS2 wird Informationssicherheit ausdrücklich zur Verantwortung der Geschäftsleitung. Die Richtlinie verlangt, dass Leitungsorgane angemessene Risikomanagementmaßnahmen genehmigen, deren Umsetzung überwachen und sich regelmäßig über deren Wirksamkeit informieren.

Entscheidend ist: Diese Verantwortung ist nicht vollständig delegierbar.

Das bedeutet nicht, dass Geschäftsführer technische Details kennen müssen. Vielmehr bedeutet es, dass sie:

- ☑ **Risiken verstehen**
- ☑ **Prioritäten setzen**
- ☑ **Ressourcen freigeben**
- ☑ **Entscheidungen dokumentieren**
- ☑ **Wirksamkeit überwachen**

Delegiert werden kann die operative Umsetzung, nicht die Verantwortung.

Im Schadensfall wird nicht nur geprüft, ob technische Maßnahmen vorhanden waren, sondern ob die Geschäftsführung ihrer Organisations- und Überwachungspflicht nachgekommen ist. Dokumentierte Risikoanalysen, beschlossene Maßnahmen, regelmäßige Reviews und nachvollziehbare Entscheidungsprotokolle sind dabei zentrale Entlastungsnachweise.

Fehlt diese Governance-Struktur, entsteht ein persönliches Haftungsrisiko, insbesondere wenn nachweisbar keine angemessene Steuerung erfolgt ist.

Hinzu kommt ein weiterer Aspekt: Cybersecurity-Versicherungen.

Versicherer prüfen zunehmend vor Vertragsabschluss und nochmal im Schadensfall, ob ein strukturiertes Informationssicherheitsmanagement existiert und gelebt wird. Ein „Papier-ISMS" reicht nicht aus. Werden vereinbarte Mindeststandards nicht eingehalten oder fehlt die dokumentierte Umsetzung, kann dies zu Leistungskürzungen oder -verweigerung führen.

Für die Geschäftsleitung bedeutet das: Informationssicherheit ist nicht nur ein IT-Risiko, sondern ein Governance- und Haftungsthema.

Nicht die Frage ***„Haben wir IT-Schutzmaßnahmen?"*** ist entscheidend, sondern:

„Können wir nachweisen, dass wir Risiken systematisch bewerten, Maßnahmen beschließen und deren Umsetzung überwachen?"

Wo diese Struktur fehlt, steigt das persönliche Risiko.
Wo sie vorhanden ist, entsteht belastbare Absicherung, regulatorisch und versicherungstechnisch.

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

NICHT DELEGIERBARE ENTSCHEIDUNGEN

Folgende Entscheidungen gelten als Managementaufgabe:

1. Festlegung des Scope (Geltungsbereich)

- ☑ Welche Geschäftsbereiche,
- ☑ Standorte und
- ☑ Prozesse werden vom Sicherheitsmanagement umfasst?

2. Risikotoleranz und Priorisierung

- ☑ Welche Risiken sind akzeptabel?
- ☑ Wo werden Investitionen priorisiert?

3. Ressourcenfreigabe

- ☑ Welche personellen und
- ☑ finanziellen Mittel werden bereitgestellt?

4. Bestellung verantwortlicher Rollen

- ☑ ISB
- ☑ Datenschutzbeauftragter
- ☑ Compliance-Funktion

5. Freigabe von Richtlinien

- ☑ Grundsatzentscheidungen zur Informationssicherheit

6. Durchführung von Management Reviews

- ☑ Regelmäßige Bewertung der Wirksamkeit des Systems

Diese Entscheidungen müssen dokumentiert sein, nicht aus formalen Gründen, sondern als Ausdruck aktiver Steuerung.

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

NACHWEISE, DIE IM ERNSTFALL SCHÜTZEN

Im Haftungsfall zählt nicht, ob theoretisch Sicherheitsmaßnahmen existierten. Entscheidend ist, ob die Geschäftsleitung nachweisen kann, dass sie ihre Organisations- und Überwachungspflicht strukturiert wahrgenommen hat.

Die folgenden Nachweise sind dabei besonders relevant:

- ☑ **Dokumentierte Risikoanalyse**
- ☑ **Beschlussprotokolle zur Maßnahmenpriorisierung**
- ☑ **Nachweis über Awareness-Programme**
- ☑ **Dokumentierte Budgetfreigaben**
- ☑ **Management-Review-Protokolle**
- ☑ **Maßnahmenstatus und Fortschrittsberichte**

Diese Dokumente erfüllen jeweils eine konkrete Schutzfunktion:

Eine dokumentierte Risikoanalyse zeigt, dass Risiken nicht ignoriert, sondern systematisch identifiziert und bewertet wurden. Sie belegt, dass Entscheidungen auf einer strukturierten Grundlage getroffen wurden – nicht zufällig oder reaktiv.

Beschlussprotokolle zur Maßnahmenpriorisierung dokumentieren, dass das Management aktiv entschieden hat, welche Risiken mit welcher Priorität behandelt werden. Gerade im Kontext begrenzter Ressourcen ist nachvollziehbare Priorisierung ein zentraler Entlastungsfaktor.

Awareness-Nachweise belegen, dass Mitarbeitende regelmäßig geschult wurden und organisatorische Sicherheitsvorgaben bekannt waren. Im Schadensfall kann dies entscheidend sein, wenn menschliches Fehlverhalten eine Rolle spielt.

Dokumentierte Budgetfreigaben zeigen, dass Informationssicherheit nicht nur formell anerkannt, sondern mit Ressourcen hinterlegt wurde. Ohne Ressourcen kann keine wirksame Risikobehandlung stattfinden.

Management-Review-Protokolle belegen die laufende Überwachung des Systems. Sie zeigen, dass Risiken regelmäßig bewertet, Maßnahmen angepasst und strategische Entscheidungen getroffen wurden.

Maßnahmenstatus- und Fortschrittsberichte dokumentieren die operative Umsetzung. Sie machen sichtbar, ob beschlossene Maßnahmen tatsächlich umgesetzt wurden oder ob offene Risiken bekannt waren und bewusst toleriert wurden.

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

Im Kern geht es nicht um die Menge der Dokumente, sondern um deren Logik:

Diese Kette muss nachvollziehbar geschlossen sein. Fehlt sie, entsteht im Ernstfall ein Beweisproblem.

Ist sie vorhanden, entsteht Governance-Nachweis und damit eine wesentliche Grundlage zur persönlichen Entlastung der Geschäftsleitung.

KPIs, REPORTING UND MANAGEMENT REVIEW

Informationssicherheit wird erst dann zur Führungsaufgabe, wenn Risiken, Fortschritte und Handlungsbedarfe regelmäßig auf Managementebene transparent gemacht werden. Geschäftsführung und Board benötigen keine technischen Detailberichte, sondern verdichtete, entscheidungsrelevante Informationen.

Typische Management-Kennzahlen sind beispielsweise:

- ☑ **offene Hochrisiken**
- ☑ **Umsetzungsgrad priorisierter Maßnahmen**
- ☑ **Status kritischer Lieferanten**
- ☑ **sicherheitsrelevante Vorfälle**
- ☑ **Awareness-Abdeckung**
- ☑ **Audit-Status**

Entscheidend ist nicht die Anzahl der Kennzahlen, sondern ihre Steuerungsrelevanz. Ein strukturiertes Reporting schafft Transparenz und dokumentiert aktive Führung.

Diese Informationen fließen in das Management Review ein. Es ist kein formaler ISO-Termin, sondern der zentrale Steuerungsmoment der Geschäftsleitung. Hier werden Risiken bewertet, Maßnahmen überprüft, Prioritäten angepasst und strategische Entscheidungen getroffen.

Ein dokumentiertes Review belegt, dass Informationssicherheit kontinuierlich überwacht und aktiv gesteuert wird. Dies ist ein wesentlicher Nachweis insbesondere im Kontext von NIS2 und möglicher Haftungsverantwortung.

KONKRETE UMSETZUNGSBAUSTEINE

1-Seiten-Board-Report (Monatsstatus ISMS)

Kompakte Übersicht für Geschäftsführung:

- ☑ Risikolage (Top 10 Risiken)
- ☑ Maßnahmenstatus
- ☑ Vorfälle
- ☑ Lieferantenstatus
- ☑ Budget / Ressourcen
- ☑ Entscheidungsbedarf

Ziel: Entscheidungsfähigkeit in 15 Minuten.

Vorlage: Management Review Agenda

Strukturierte Agenda mit:

1. Status Risikomanagement
2. Maßnahmenfortschritt
3. Vorfälle
4. Lieferkette
5. Ressourcen
6. Beschlüsse & Prioritäten

Damit wird das Review zum aktiven Steuerungsinstrument – nicht zur Formalität.

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

FAZIT

Informationssicherheit ist heute eine unternehmerische Kernverantwortung. Regulatorische Anforderungen machen deutlich: **Die Geschäftsleitung trägt die Organisationspflicht.**

Haftung entsteht nicht durch Vorfälle allein. Haftung entsteht durch fehlende Steuerung.

Unternehmen, die:

- ☑ **Risiken systematisch bewerten**
- ☑ **Entscheidungen dokumentieren**
- ☑ **Maßnahmen priorisieren**
- ☑ **regelmäßig berichten**
- ☑ **Management-Reviews durchführen**

schaffen belastbare Governance.

Die entscheidende Frage für Geschäftsführer lautet daher nicht: *„Sind wir 100 % sicher?"*

Sondern: *„Können wir nachweisen, dass wir unsere Verantwortung strukturiert wahrnehmen?"*

Wo Governance transparent ist, sinkt das Haftungsrisiko. Wo sie fehlt, entsteht Unsicherheit.

Der nächste Schritt ist klar: Sicherheitsmanagement zur Chefsache machen, strukturiert, dokumentiert und steuerbar.