VANTARION

BIA & RISIKO-MANAGEMENT

Vom Geschäftsprozess zum Restrisiko

Ein Praxisleitfaden für
Geschäftsführung, ISB, Compliance & IT-Leitung

MANAGEMENT SUMMARY

Risikomanagement in der Informationssicherheit ist keine Excel-Übung und kein rein technisches Thema. Es ist ein strukturierter Entscheidungsprozess, der Geschäftsrisiken transparent macht und Prioritäten festlegt.

Eine Business Impact Analysis (BIA) bildet die Grundlage. Sie klärt, welche Prozesse für das Unternehmen kritisch sind und welche Auswirkungen ein Ausfall hätte. Darauf aufbauend identifiziert das Risikomanagement konkrete Szenarien, bewertet Eintrittswahrscheinlichkeit und Schadensausmaß und leitet geeignete Maßnahmen ab.

Ein belastbares System beantwortet drei Kernfragen:

- ☑ **Welche Geschäftsprozesse sind kritisch?**
- ☑ **Welche Risiken bedrohen diese Prozesse?**
- ☑ **Welche Maßnahmen reduzieren das Risiko** auf ein akzeptables Niveau?

Dieses Whitepaper beschreibt eine praxiserprobte Vorgehensweise, die den Anforderungen aus ISO 27001, ISO 27005, ISO 27002, NIS2 und TISAX entspricht – ohne unnötige Komplexität.

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.

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

DIE BIA – AUSWIRKUNGEN VERSTEHEN

Die Business Impact Analysis ist der erste Schritt. Sie bewertet nicht, wie wahrscheinlich ein Schaden ist, sondern wie schwerwiegend er wäre.

Im Fokus stehen die Geschäftsprozesse.

Für jeden relevanten Prozess werden die Auswirkungen bewertet, bei Verlust von:

- ☑ **Vertraulichkeit**
- ☑ **Integrität**
- ☑ **Verfügbarkeit**

Diese Bewertung erfolgt aus Geschäftssicht: Welche finanziellen, regulatorischen oder reputativen Folgen hätte ein Ausfall? Welche Zeiträume sind tolerierbar?

Das Ergebnis ist eine Priorisierung der Prozesse nach Kritikalität. Ohne BIA fehlt die Grundlage für jede sinnvolle Risikoentscheidung.

DIE SYSTEMLOGIK: VIER OBJEKTE

Ein strukturiertes Risikomodell basiert auf vier miteinander verknüpften Elementen:

- ☑ **Prozesse**
- ☑ **Assets**
- ☑ **Szenarien**
- ☑ **Maßnahmen**

Diese Trennung schafft Transparenz und verhindert Vermischung von Geschäfts- und Techniklogik.

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

2.1 Prozesse

Prozesse sind die geschäftliche Ebene.

Beispiele:

- ☑ Auftragsabwicklung
- ☑ Produktion
- ☑ Kundenportal
- ☑ Abrechnung
- ☑ Entwicklung

Für jeden Prozess wird festgelegt:

- ☑ Kritikalität in Bezug auf Vertraulichkeit
- ☑ Kritikalität in Bezug auf Integrität
- ☑ Kritikalität in Bezug auf Verfügbarkeit

Die höchste Auswirkung bestimmt den Business Impact.

2.2 Assets

Assets sind alle Werte, die zur Durchführung eines Prozesses benötigt werden.

Dazu zählen:

- ☑ IT-Systeme
- ☑ Anwendungen
- ☑ Daten
- ☑ Infrastruktur
- ☑ Personal
- ☑ Dienstleister

Jedes Asset erhält:

- ☑ **eine eigene Vertraulichkeits-, Integritäts- und Verfügbarkeitsbewertung**
- ☑ **einen verantwortlichen Asset Eigentümer**
- ☑ **einen verantwortlichen Risiko Eigentümer**

Wichtig: Die Bewertung erfolgt zunächst ohne Berücksichtigung vorhandener Maßnahmen.

2.3 Szenarien

Szenarien beschreiben konkrete Gefährdungssituationen.

Typische Beispiele:

- ☑ **Ransomware**
- ☑ **Datenmanipulation**
- ☑ **Fehlkonfiguration**
- ☑ **Ausfall eines Cloud-Dienstleisters**
- ☑ **Insider-Missbrauch**
- ☑ **physischer Schaden**

Für jedes Szenario werden bewertet:

- ☑ **Eintrittswahrscheinlichkeit**
- ☑ **Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit**

Wichtig: Die Bewertung erfolgt zunächst ohne Berücksichtigung vorhandener Maßnahmen.

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

RISIKOBILDUNG

Ein Risiko ergibt sich aus der Kritikalität eines Geschäftsprozesses, der Betroffenheit der zugehörigen Assets und der Wahrscheinlichkeit eines konkreten Schadensszenarios.

Je höher die geschäftlichen Auswirkungen und je wahrscheinlicher ein Ereignis, desto höher ist das Risiko.

Das Initialrisiko beschreibt dabei die Ausgangslage, also das Risiko ohne Berücksichtigung bestehender Schutzmaßnahmen.

MASSNAHMEN

Maßnahmen wirken auf zwei Ebenen:

1. **Reduktion der Eintrittswahrscheinlichkeit: z. B. durch MFA, Patch-Management, Zugriffskontrollen**

2. **Reduktion der Schadensauswirkung: durch Backups, Notfallkonzepte, Monitoring**

Jede Maßnahme sollte bewertet werden hinsichtlich:

- ☑ **Wirksamkeit auf Wahrscheinlichkeit**
- ☑ **Wirksamkeit auf Auswirkung (Vertraulichkeit, Integrität, Verfügbarkeit)**
- ☑ **Implementierungsstatus**

Der Implementierungsstatus ist entscheidend:

- ☑ **nicht umgesetzt = keine Wirkung**
- ☑ **teilweise umgesetzt = reduzierte Wirkung**
- ☑ **vollständig implementiert = volle Wirkung**

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

RESTRISIKO UND RISIKOTOLERANZ

Sobald Szenarien, Assets und Geschäftsprozesse miteinander verknüpft und die vorhandenen Maßnahmen berücksichtigt wurden, entsteht ein realistisches Bild der verbleibenden Risiken.

Maßnahmen wirken dabei auf unterschiedliche Ebenen. Sie können...

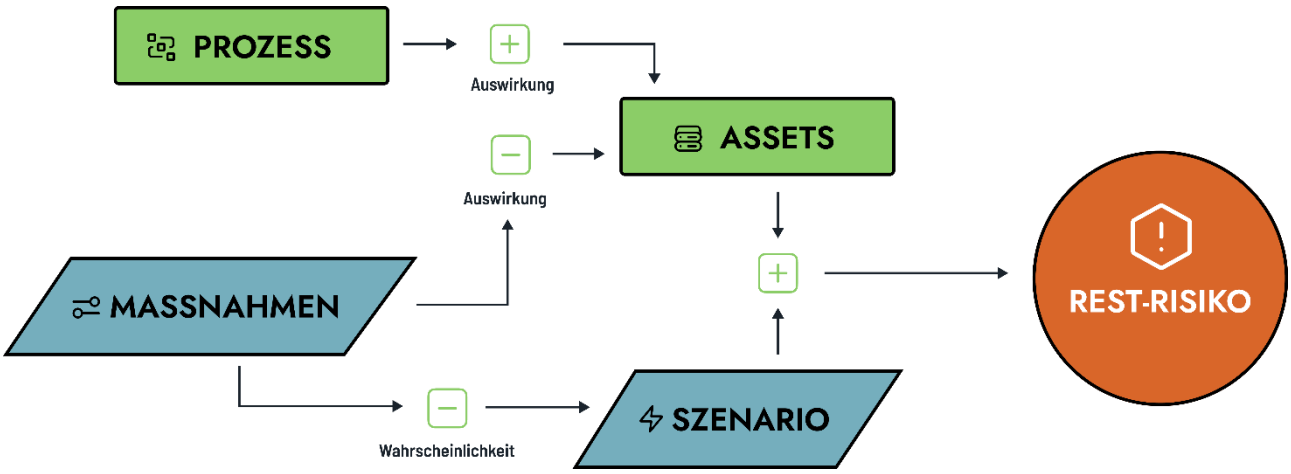
- ☑ **die Eintrittswahrscheinlichkeit eines Szenarios reduzieren oder**
- ☑ **dessen Auswirkungen auf ein Asset begrenzen.**

Durch diese Verknüpfung verändert sich das ursprüngliche Risikobild.

Das verbleibende Risiko, also das Risiko nach Berücksichtigung der bestehenden Schutzmaßnahmen, wird als Restrisiko bezeichnet.

Dieses Restrisiko wird nicht isoliert betrachtet, sondern im Verhältnis zur definierten Risikotoleranz des Unternehmens bewertet. Die Risikotoleranz legt fest, welches Risikoniveau akzeptabel ist und ab welchem Punkt weitere Maßnahmen erforderlich werden.

Die Entscheidung, ob ein Restrisiko akzeptiert oder weiter reduziert werden soll, ist keine technische Detailfrage, sondern eine bewusste Managemententscheidung.



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

FOKUS: DIE KRITISCHSTEN ASSETS

In der Praxis empfiehlt sich die Konzentration auf bspw. die 10 Assets mit dem höchsten Restrisiko.

Für diese Assets wird analysiert:

- ☑ **Welche Szenarien treiben das Risiko?**
- ☑ **Welche Maßnahmen sind unzureichend?**
- ☑ **Besteht Handlungsbedarf?**
- ☑ **Oder ist das Risiko akzeptabel?**

Diese Analyse bildet die Grundlage für Priorisierung und Budgetplanung.

VERKNÜPFUNG MIT ISO 27002

ISO 27002 liefert den Maßnahmenkatalog. Diese werden nicht isoliert umgesetzt, sondern risikobasiert ausgewählt. Das bedeutet:

- ☑ **Kein pauschales „Alles implementieren"**
- ☑ **Keine isolierten Einzelmaßnahmen**
- ☑ **Sondern gezielte Auswahl basierend auf bewerteten Risiken**

Damit wird das Risikomanagement zur Steuerungsgrundlage des ISMS.

INTEGRATION IN DAS MANAGEMENTSYSTEM

BIA und Risikomanagement sind kein einmaliges Projekt. Regelmäßige Aktualisierung ist erforderlich bei:

- ☑ **neuen Systemen**
- ☑ **neuen Prozessen**
- ☑ **geänderten Bedrohungslagen**
- ☑ **Vorfällen**
- ☑ **regulatorischen Änderungen**

Die Ergebnisse fließen in:

- ☑ **Maßnahmenplanung**
- ☑ **Budgetentscheidungen**
- ☑ **Management Review**
- ☑ **strategische Ausrichtung**

Damit wird Risikomanagement zu einem aktiven Steuerungsinstrument.

Noch einfacher? Geht auch!

Man muss nicht alles selbst machen. Sie als Entscheider in einem KMU wissen, welche Kompetenzen Sie wo am sinnvollsten nutzen. Wir bei Vantarion wissen um Informationssicherheit, gesetzliche Anforderungen und wie auch Ihr Unternehmen beides vereinen kann.

Weitere Informationen auf unserer Website https://www.vantarion.de

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

FAZIT

Eine strukturierte Business Impact Analysis und ein nachvollziehbares Risikomanagement schaffen Transparenz über die tatsächlichen Risiken eines Unternehmens. Sie verbinden Geschäftsprozesse, Assets und konkrete Szenarien zu einem belastbaren Gesamtbild und machen deutlich, wo Handlungsbedarf besteht und wo Risiken bewusst getragen werden können.

Entscheidend ist dabei nicht die Menge an Bewertungen oder Maßnahmen, sondern die klare Systemlogik:

Wer diesen Zusammenhang sauber aufbaut und regelmäßig überprüft, erfüllt nicht nur normative Anforderungen aus ISO 27001, ISO 27005, ISO 27002, NIS2 oder TISAX. Er schafft eine fundierte Entscheidungsgrundlage für Priorisierung, Budgetierung und strategische Ausrichtung.

Risikomanagement ist damit kein isoliertes Sicherheitsprojekt, sondern ein kontinuierlicher Steuerungsprozess, getragen vom Management, umgesetzt in der Organisation und regelmäßig überprüft.

Erst wenn Restrisiken bewusst bewertet und entschieden werden, wird Informationssicherheit zu einer unternehmerischen Aufgabe.

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