VANTARION

Sicherheitsbasis für KMU

Die 20 Kontrollen, die 80 % Risiko reduzieren

Ein Praxisleitfaden für
IT-Leitung & Geschäftsführung

MANAGEMENT SUMMARY

Viele mittelständische Unternehmen befinden sich in einer ähnlichen Situation:

Die Bedrohungslage steigt sichtbar. Kunden stellen konkrete Sicherheitsanforderungen. Versicherer prüfen Voraussetzungen für Cyber-Deckungen. Gleichzeitig fehlt häufig die Zeit, ein vollständiges Managementsystem von Grund auf aufzubauen.

Die zentrale Frage lautet daher nicht:
„Wie erfüllen wir jede einzelne Normanforderung?"

Sondern:
„Wo erzielen wir mit vertretbarem Aufwand die größte Risikoreduktion?"

Die Erfahrung aus Incident-Analysen, Penetrationstests und Audits zeigt deutlich: Die Mehrheit erfolgreicher Angriffe nutzt grundlegende Schwächen. Fehlende Mehrfaktor-Authentifizierung, überprivilegierte Administratorrechte, ungetestete Backups oder nicht geschlossene Sicherheitslücken sind die häufigsten Ursachen.

Wer diese Basis sauber absichert, reduziert einen Großteil des realen Risikos – häufig weit mehr als durch punktuelle Einzelmaßnahmen oder isolierte Speziallösungen.

Dieses Whitepaper beschreibt:

- ☑ **welche 20 Kernkontrollen eine belastbare Sicherheitsbasis schaffen,**
- ☑ **in welcher Reihenfolge sie sinnvoll eingeführt werden sollten,**
- ☑ **welche Abhängigkeiten zu beachten sind,**
- ☑ **und wie die Umsetzung auditfähig dokumentiert wird.**

Ziel ist kein theoretisches Idealmodell, sondern eine robuste, priorisierte und realistisch umsetzbare Sicherheitsarchitektur für KMU.

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

WARUM EINE STRUKTURIERTE SICHERHEITSBASIS ENTSCHEIDEND IST

ISO 27001, NIS2 und andere Normen beschreiben ein ganzheitliches Managementsystem. Zuerst entsteht die Governance-Struktur, sie schafft Klarheit über Verantwortung und Prioritäten. Auf dieser Basis werden technische Kontrollen gezielt und risikoorientiert implementiert.

Governance definiert also das ***„Warum" und „Wofür".***

Die technische Sicherheitsbasis liefert das ***„Wie".***

Ohne klare Verantwortlichkeiten, definierte Entscheidungswege und priorisierte Risikobetrachtung entstehen technische Einzelmaßnahmen ohne strategische Steuerung. Umgekehrt bleibt Governance wirkungslos, wenn keine operative Substanz vorhanden ist.

Eine strukturierte Sicherheitsbasis erfüllt daher drei zentrale Funktionen:

1. Sie reduziert reale Angriffsflächen: **Grundlegende Schwachstellen werden systematisch geschlossen.**

2. Sie schafft operative Stabilität: **Wiederherstellungsfähigkeit und Reaktionsfähigkeit werden erhöht.**

3. Sie macht Governance wirksam: **Erst durch implementierte Kontrollen werden Prioritäten messbar und steuerbar.**

Die hier beschriebenen 20 Kontrollen sind deshalb nicht als Ersatz für Governance zu verstehen, sondern als deren operative Umsetzungsebene. Sie bilden die technische Grundlage, auf der ein wirksames ISMS aufgebaut und kontinuierlich weiterentwickelt werden kann.

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

DIE 20 KERNKONTROLLEN – STRATEGISCH GEGLIEDERT

Die nachfolgenden Maßnahmen sind nicht zufällig gewählt. Sie orientieren sich an realen Angriffsszenarien und an den Kontrollbereichen der ISO 27001 (Technologie, Organisation, Personal, Physisch).

1. Identität & Zugriff – Der häufigste Angriffsvektor

Die Mehrheit moderner Angriffe beginnt mit kompromittierten Zugangsdaten. Deshalb steht Identitätskontrolle an erster Stelle.

Eine wirksame Basis umfasst:

- ☑ **Verpflichtende Multi-Faktor-Authentifizierung (MFA) für alle extern erreichbaren Systeme, besonders für administrative Konten**
- ☑ **Strikte Trennung zwischen Benutzer- und Administratorrechten**
- ☑ **Zentrale Benutzerverwaltung mit klarer Rollenstruktur und regelmäßiger Überprüfung**

Diese Maßnahmen reduzieren das Risiko kompromittierter Accounts erheblich. Gleichzeitig schaffen sie Transparenz über privilegierte Zugriffe ein zentrales Prüfkriterium in nahezu jedem Audit.

2. Patch- & Schwachstellenmanagement – Systematische Härtung

Ungepatchte Systeme zählen weiterhin zu den häufigsten Einfallstoren.

Eine strukturierte Herangehensweise umfasst:

- ☑ **Dokumentierten Patch-Prozess mit definierten Fristen nach Kritikalität**
- ☑ **Regelmäßige automatisierte Schwachstellenscans**
- ☑ **Härtungsrichtlinien für Server und Clients**

Wichtig ist weniger die absolute Geschwindigkeit, sondern die Nachvollziehbarkeit: Welche Systeme sind betroffen? Wer ist verantwortlich? Wann erfolgt die Aktualisierung?

Ein geregelter Patch-Prozess ist eines der zentralen Elemente jeder technischen Sicherheitsbasis.

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

3. Backup & Resilienz – Die letzte Verteidigungslinie

Kein System ist vollständig unangreifbar. Deshalb ist Wiederherstellungsfähigkeit entscheidend.

Eine belastbare Backup-Strategie umfasst:

- ☑ **Automatisierte Sicherungen mit definierten Intervallen**
- ☑ **Trennung von Backup-Systemen und -Administratoren**
- ☑ **Eine Offline- oder Immutable-Backup-Komponente**
- ☑ **Regelmäßige dokumentierte Wiederherstellungstests**

Ransomware-Vorfälle zeigen deutlich: Backups sind nur dann wirksam, wenn sie technisch isoliert und regelmäßig getestet sind.

Die Kombination aus Schutz und Wiederherstellungsfähigkeit bildet die Grundlage operativer Resilienz.

4. Endpoint- & Netzwerksicherheit – Sichtbarkeit herstellen

Sicherheit bedeutet nicht nur Prävention, sondern auch Erkennung.

Eine wirksame Basis umfasst:

- ☑ **Endpoint Protection mit Detection & Response (EDR)**
- ☑ **Zentrale Protokollierung sicherheitsrelevanter Ereignisse**
- ☑ **Regelmäßige Überprüfung von Firewall-Regeln**
- ☑ **Netzwerksegmentierung**

Ohne Protokollierung bleibt ein Angriff häufig unentdeckt. Ohne Segmentierung breitet er sich unkontrolliert aus. Transparenz ist Voraussetzung für wirksame Reaktion.

5. Mobile & Remote-Sicherheit – Arbeitsrealität absichern

Mobile Endgeräte und Remote-Zugriffe erhöhen die Komplexität.

Zur Basis gehören:

- ☑ **Mobile Device Management**
- ☑ **Verpflichtende Geräteverschlüsselung**
- ☑ **Richtlinien für sichere Heimarbeitsplätze**
- ☑ **Zugriff ausschließlich über abgesicherte VPN- oder Zero-Trust-Lösungen**

Geräteverlust, unsichere WLANs oder ungeschützte Laptops stellen reale Risiken dar, die systematisch adressiert werden müssen.

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

6. Organisatorische Mindeststruktur – Technik ergänzen

Technische Maßnahmen entfalten ihre Wirkung nur, wenn organisatorische Strukturen vorhanden sind.

Unverzichtbar sind:

- ☑ **Dokumentierter und geschulte Incident-Response-Prozess mit klaren Meldewegen**
- ☑ **Regelmäßige Awareness-Schulungen für Mitarbeiter**

Ein definierter Vorfallprozess reduziert Reaktionszeiten und begrenzt Schäden. Awareness reduziert das Risiko menschlicher Fehlhandlungen erheblich. Technik ohne Organisation bleibt unvollständig.

REIHENFOLGE UND ABHÄNGIGKEITEN

Die Einführung der 20 Kontrollen sollte strukturiert erfolgen.

Empfohlene Logik:

1. Identitäten absichern: **Zugangskontrolle herstellen**
2. Systeme härten: **Schwachstellen schließen**
3. Resilienz aufbauen: **Wiederherstellungsfähigkeit sicherstellen**
4. Überwachung etablieren: **Sichtbarkeit schaffen**
5. Organisation ergänzen: **Prozesse und Schulungen integrieren**

Diese Reihenfolge verhindert, dass isolierte Einzelmaßnahmen ohne Gesamtwirkung eingeführt werden.

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

NACHWEISFÜHRUNG – VON DER TECHNIK ZUR AUDITFÄHIGKEIT

Technische Umsetzung allein genügt nicht. Im Audit zählt die Steuerbarkeit.

Für jede Maßnahme müssen folgende Punkte nachvollziehbar dokumentiert sein:

- ☑ Ziel und Risikobezug
- ☑ Implementierungsstatus
- ☑ Verantwortliche Rolle
- ☑ Überprüfungsintervall
- ☑ Dokumentierter Nachweis

Beispielsweise:

- ☑ Screenshot aktivierter MFA
- ☑ Protokoll eines Restore-Tests
- ☑ Bericht eines Schwachstellenscans
- ☑ Teilnahmeprotokoll einer Awareness-Schulung

Erst durch strukturierte Dokumentation entsteht Auditfähigkeit.

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

PRAXISVORLAGEN & STEUERUNGSINSTRUMENTE

Umsetzungscheckliste

Diese Checkliste dient als operatives Steuerungsinstrument.

Sie enthält für jede Kontrolle:

- ☑ Priorität
- ☑ Verantwortliche Rolle
- ☑ Status
- ☑ Fristen
- ☑ Prüffrequenz
- ☑ Nachweisart

Sie ermöglicht Transparenz für IT-Leitung und Geschäftsführung.

Template: IT-Sicherheitsmaßnahmen-Protokoll

Das Maßnahmenprotokoll verbindet technische Umsetzung mit Management-Steuerung.

Es dokumentiert:

- ☑ Maßnahme
- ☑ Ziel
- ☑ Bezug zu identifiziertem Risiko
- ☑ Implementierungsdatum
- ☑ Verantwortliche Person
- ☑ Überprüfungstermin
- ☑ Nachweisform

Dieses Protokoll bildet die Grundlage für Reporting, Audits und kontinuierliche Verbesserung.

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

FAZIT

Eine belastbare Sicherheitsbasis entsteht nicht durch Komplexität, sondern durch Priorisierung.

Wer diese 20 Kontrollen strukturiert umsetzt, erreicht:

- ☑ **signifikante Reduktion realer Angriffsrisiken**
- ☑ **höhere Resilienz gegenüber Ransomware und Datenverlust**
- ☑ **bessere Voraussetzungen für Cyber-Versicherungen**
- ☑ **Anschlussfähigkeit an ISO 27001, NIS2 oder vergleichbare Normen**
- ☑ **fundierte Grundlage für ein strukturiertes ISMS**

Sicherheit beginnt nicht mit einem Zertifikat. Sie beginnt mit klar priorisierten, wirksamen Kontrollen.

Wer diese Basis sauber aufsetzt, schafft nicht nur „schnelle Verbesserung", sondern eine nachhaltige Sicherheitsarchitektur für die kommenden Jahre.