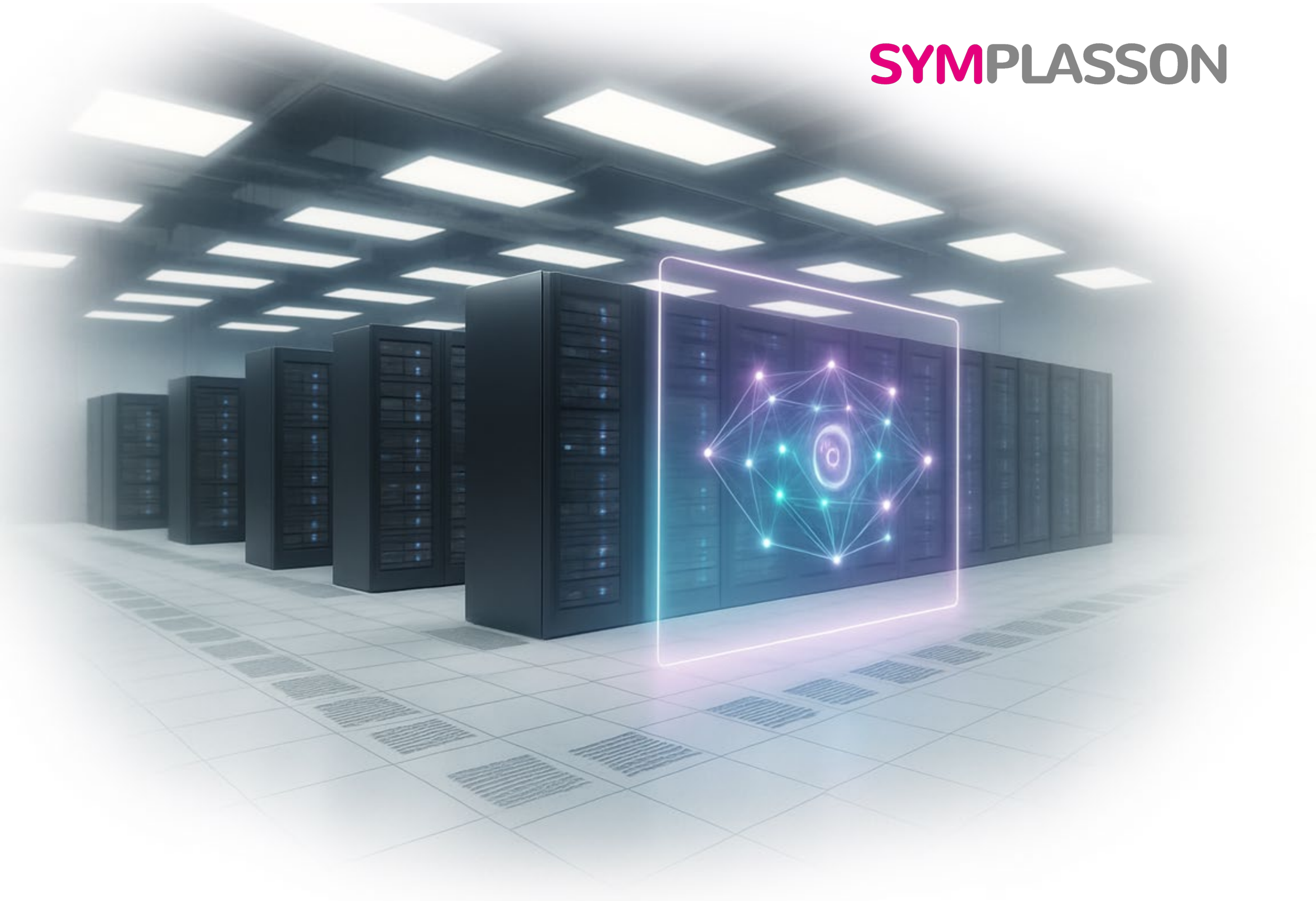
SYMPLASSON



DIGITALE RESILIENZ IM MITTELSTAND

Warum Managed IT Security heute Betriebswirtschaftliche Pflicht ist

Digitale Risiken verschwinden nicht – aber sie lassen sich steuern. Dieses Whitepaper zeigt, wie mittelständische Unternehmen Cyberrisiken aus der IT-Ecke holen und zu einem Führungswerkzeug machen: für Stabilität, Nachweisbarkeit und nachhaltige Geschäftssicherheit.

Jeger, Dennis
djeger@symplasson.de

Inhalt

Digitale Stabilität als Voraussetzung für Unternehmensführung	2
Problem – Status Quo	3
Executive-Perspektive: Nicht Technik. Unternehmenssteuerung	4
Risikoreduktion ist eine Finanzfunktion	5
Der ökonomische Kern	6
Kostenmechanik eines Sicherheitsvorfalls	7
Lösung: Sicherheitsbetrieb statt Tool-Kauf	8
Rollenmodell in der Praxis: Gemeinsame Sicherheitsführung	9
Wirtschaftliche Leitfrage	10
ROI-Modell: Sicherheitsbetrieb vs. Störkosten	11
Governance statt Hoffnung	12
SYMPLASSON-Modell: Sicherheitsbetrieb im Mittelstand	13
Praxisfall: Der Unterschied zwischen Krise und Kontrolle	14
Kennzahlen, die im Mittelstand wirklich zählen	15
Verfügbarkeits- und Governance-Kennzahlen	16
Reifegradmodell und Handlungsschritte	17
Haftung & Compliance – der leise, harte Faktor	18
Der wahre Wert: Stabilitätskultur	19
Fazit	20
Kontakt	21

Digitale Stabilität als Voraussetzung für Unternehmensführung

Digitale Stabilität ist zur zentralen Voraussetzung mittelständischer Wertschöpfung geworden. Unternehmen sind heute nicht mehr durch Kapital oder Personal limitiert, sondern durch ihre Fähigkeit, digitale Unterbrechungen zu verhindern oder kontrolliert zu bewältigen. Die meisten mittelständischen Organisationen betreiben IT effizient – aber Sicherheit nur fragmentiert. Dadurch entsteht ein strukturelles Risiko: Technologie wächst schneller als die Fähigkeit, sie gegen Angriffe abzusichern.

Cyberrisiken sind deshalb keine technischen Ereignisse, sondern betriebswirtschaftliche Risiken. Sie bedrohen Cashflow, Kundenvertrauen, Steuerungsfähigkeit und im Worst Case die Existenz. Das Ziel ist nicht, jeden Angriff zu verhindern — sondern sicherzustellen, dass ein Angriff nicht zum Geschäftsereignis wird. Entscheidend ist die Fähigkeit, Abweichungen früh zu erkennen, kontrolliert zu reagieren und Betriebsfähigkeit nachweislich aufrechtzuerhalten. Diese Fähigkeit entsteht nicht durch den Kauf einzelner Sicherheitsprodukte, sondern durch einen kontinuierlichen Sicherheitsbetrieb:

Kontinuierlicher Betrieb

Überwachung, Priorisierung und Reaktion in Echtzeit

Klare Verantwortung

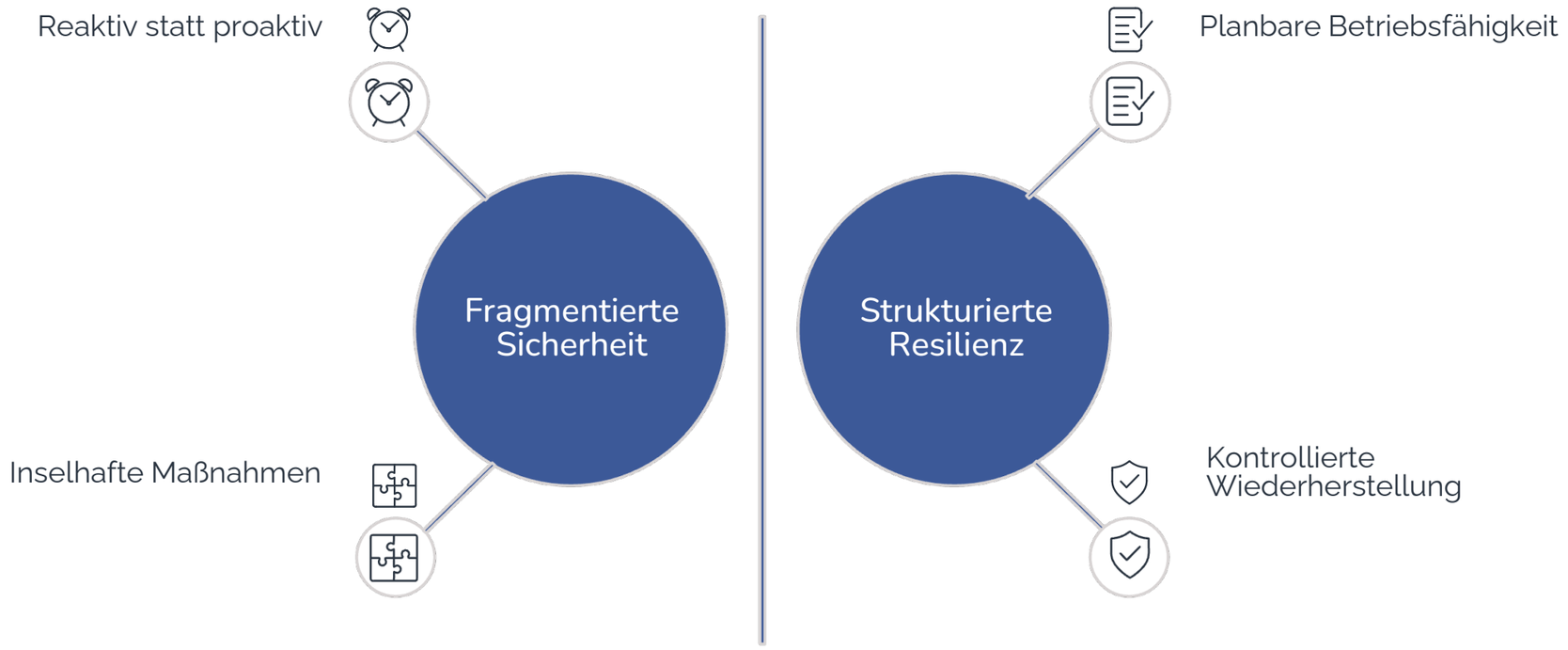
Definierte Prozesse und dokumentierte Zuständigkeiten

Messbare Resilienz

Planbare, steuerbare und auditfähige Sicherheit

Managed IT Security ermöglicht es mittelständischen Unternehmen, diese Betriebsfunktion aufzubauen, ohne eigene Ressourcen zu überlasten oder Spezialkapazitäten dauerhaft vorzuhalten. Die interne IT bleibt produktiver Kern der Wertschöpfung — die Sicherheitsbetriebsfähigkeit wird professionell ergänzt. Das Ergebnis ist nicht „mehr IT-Sicherheit", sondern planbare digitale Stabilität. Statt reaktiver Brandbekämpfung entsteht messbare, steuerbare und auditfähige Resilienz.

> Managed Security sichert keine Systeme – sie sichert Geschäftsfähigkeit.



Problem – Status Quo

Unternehmen scheitern nicht, weil sie angegriffen werden. Sie scheitern, weil sie zu spät reagieren.

Wer heute ein mittelständisches Unternehmen führt, steuert nicht mehr nur Kapital, Personal und Lieferketten. Digitale Stabilität ist stille Infrastruktur – kein Vorteil, sondern Grundvoraussetzung für Liquidität, Reputation und Vertragsfähigkeit. Unternehmen, die noch argumentieren „Unsere IT läuft – wir sind sicher", befinden sich in derselben Denkfalle wie Betriebe, die früher sagten „Wir haben keine Konkurrenz – unsere Kunden bleiben."

Digitalwirtschaft straft Selbstzufriedenheit härter ab als jeder Markt. Systeme, die funktionieren, beweisen keinen Schutz — sie beweisen lediglich Glück. Führung, die auf Glück baut, führt Risiko, nicht Organisation.

Die Herausforderung ist daher nicht technischer Natur, sondern eine Frage der Steuerungsfähigkeit: Erkennen, bewerten, reagieren, wiederherstellen — bevor ein technisches Ereignis zu einer betriebswirtschaftlichen Krise eskaliert.

Executive-Perspektive: Nicht Technik. Unternehmenssteuerung.

Den CFO interessiert selten Malware.

Er interessiert sich für Cashflow, Planbarkeit und Durchhaltefähigkeit.

Cyberrisiken sind Liquiditäts-, Vertrags- und Reputationsrisiken. Security ist Finanz- und Unternehmenssteuerung, nicht Technik.

Digitale Sicherheit ist deshalb ein Bestandteil moderner Unternehmenssteuerung: Risiken sichtbar machen, Erwartungswerte kontrollieren, Finanzschäden vermeiden und Lieferfähigkeit sichern. Sicherheitsbetrieb ist Finanzführung durch Stabilität. Nicht „mehr IT", sondern beherrschbare Betriebsrisiken.

Worauf Entscheider wirklich schauen:

Strategischer Fokus	Management-Frage
Umsatzsicherheit	Können wir auch bei Störungen produzieren, liefern, fakturieren?
Schutz digitaler Vermögenswerte (CapEx)	Sind unsere Investitionen in Systeme, Daten und Infrastruktur werthaltig abgesichert?
Kosten und Aufwandsplanbarkeit (OpEx)	Können wir Sicherheitsaufwand planbar machen, statt Krisenkosten zu tragen?
Risikokapitalbindung	Wie viel Liquidität setzen wir bei einem Vorfall aufs Spiel?
Vertrags- & Lieferpflichten	Vermeide ich Vertragsstrafen & SLA-Brüche?

Risikoreduktion ist eine Finanzfunktion

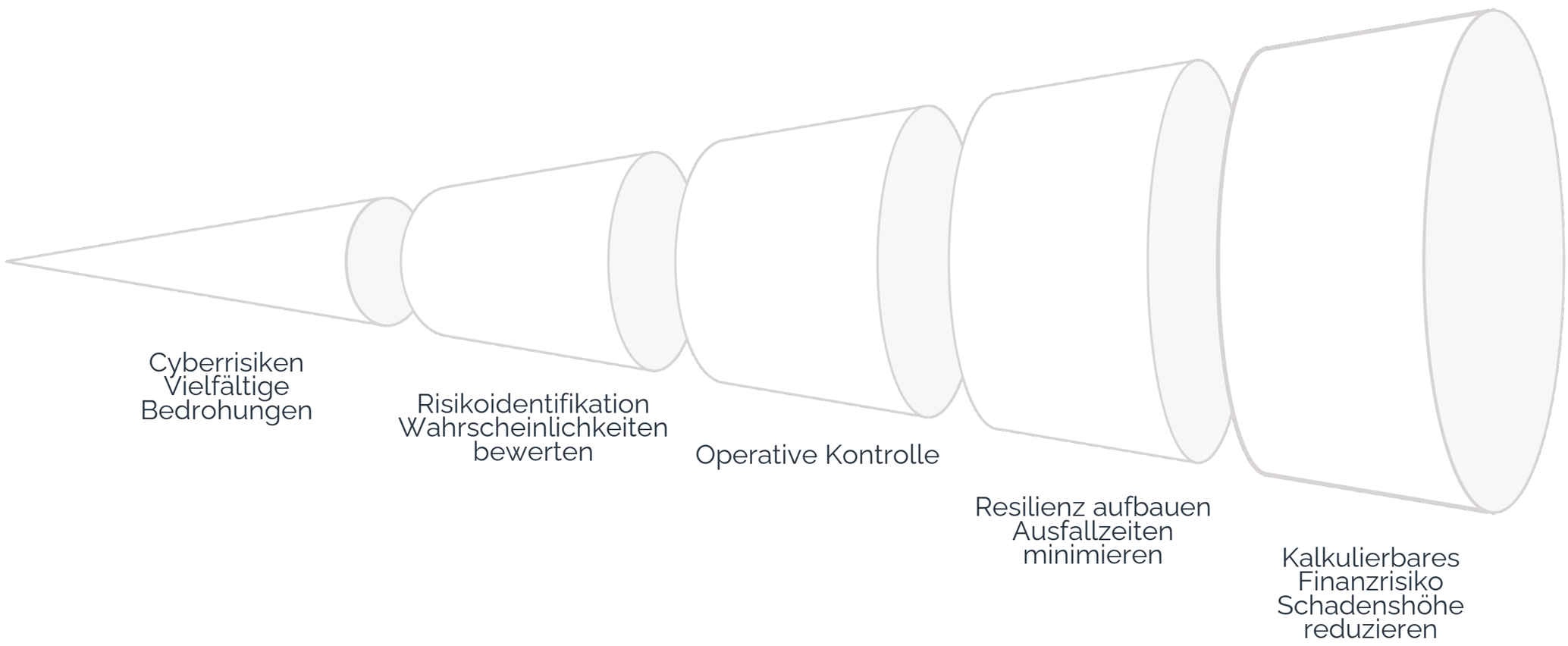
In klassischen Finanzmodellen wird Risiko verstanden als Verhältnis von Eintrittswahrscheinlichkeit und potenzieller Schadenshöhe. In der digitalen Realität verschiebt sich dieser Ansatz: Cyberrisiken lassen sich nicht vollständig quantifizieren, sie lassen sich nur operationalisieren.

Unternehmen scheitern nicht, weil sie angegriffen werden. Sie scheitern, weil sie zu spät reagieren, keine Wiederanlaufmechanismen haben und der Angriff in eine betriebswirtschaftliche Krise eskaliert. Damit wird Security zur Parallele von Liquiditätsmanagement: Nicht die Erwartung eines Problems entscheidet, sondern die Fähigkeit, es ohne strukturellen Schaden zu überstehen.

1	2	3
Risiko erkennen	**Kontrolle aufbauen**	**Wert schützen**
Digitale Bedrohungen identifizieren	Wiederherstellungsfähigkeit sichern	Kapitalvernichtung vermeiden

Moderne Unternehmensführung bewertet daher weniger die „Gefahr" als die Kontroll- und Wiederherstellungsfähigkeit. Genau hier liegt die wirtschaftliche Rechtfertigung für Managed Security: Sicherheit ist kein Aufwand. Sicherheit ist die Reduktion des kapitalvernichtenden Zufalls.

> Unternehmen, die digitale Risiken aktiv steuern, können kalkulieren. Unternehmen, die sie ignorieren, spekulieren.



Der ökonomische Kern

Sicherheitsbetrieb ist ein Instrument zur Optimierung von Erwartungswerten. Ziel ist nicht maximale Abschottung, sondern maximale Steuerbarkeit und minimale Störkosten. Nicht Verteidigung um jeden Preis, sondern kontrollierte Betriebsfähigkeit unter Unsicherheit.

Erwarteten Schaden minimieren

Risiko × Eintrittswahrscheinlichkeit – Reduktion durch geübte Prozesse.

Steuerbarkeit erhöhen

Messbare Reduktion von Volatilität im Geschäftsbetrieb.

Unternehmenswert steigern

Volatilität ist das Gegenteil von Wert und muss reduziert werden.

Ökonomisch betrachtet entsteht Wert dort, wo Risiko messbar reduziert und Wiederanlauffähigkeit gesichert wird. Ein CEO bewertet dabei Kernfragen:

- → Kann ich meine Leistung dauerhaft liefern?
- → Welche Störungskosten drohen?
- → Sind meine Risiken haftungs- und reputationsfähig adressiert?
- → Ist meine IT planbar – oder volatil?

Sicherheit ist die Reduktion von Volatilität. Und Volatilität ist das Gegenteil von Unternehmenswert.

Kostenmechanik eines Sicherheitsvorfalls

Die Frage ist nie, ob ein Angriff passiert. Die Frage ist: Wie tief greift er in Wertschöpfung und Liquidität ein?

Ein Sicherheitsvorfall ist in erster Linie ein betriebswirtschaftliches Ereignis, kein technisches. Die Kosten entstehen durch Stillstand, Unsicherheit, Zeitverlust und Führungsfokusverschiebung.

Kostenebenen eines Vorfalls

Direkte Kosten

- Forensik & externe Experten
- Wiederherstellung & Datenbereinigung
- Rechts- & Meldepflichten
- Notfallmaßnahmen & Sofortreaktionen

Indirekte Kosten

- Produktions-/Lieferausfälle
- Verzögerte Fakturierung / Umsatzausfälle
- Kunden- & Vertrauensverlust
- Projektstopps & verschobene Initiativen
- Führung: Krisen- vs. Wertschöpfung

Strategische Kosten

- IT-Team-Überlastung & Burnout
- Entscheidungsunsicherheit & Prioritätschaos
- Innovations- & Investitionsstau
- Reputationsrisiken (Markt, Lieferkette, Aufsichtsrat)

Falsche Denkweise

„Security kostet Geld und bremst."

Richtige Denkweise

„Security reduziert Risikoexposition, Stabilitätskosten und Opportunitätsverluste."

Cyberangriff = Betriebsunterbrechung + Marktvertrauensverlust. In keinem Geschäftsmodell ist das tragbar.

Lösung: Sicherheitsbetrieb statt Tool-Kauf

Ein Mittelstandsunternehmen braucht keine Hackerarmee. Es braucht ein Betriebsmodell, das vier Fähigkeiten dauerhaft sicherstellt:

Erkennen

Verhindert wirtschaftliche Relevanz von Angriffen durch frühzeitige Identifikation

Reagieren

Minimiert Dauer & Eingriffstiefe durch schnelle, koordinierte Maßnahmen

Wiederherstellen

Wandelt Totalschaden in Störung durch geübte Wiederanlaufprozesse

Steuern & Nachweisen

Schafft planbare Stabilität durch messbare Prozesse und Dokumentation

Nicht Tools, sondern Betriebsfähigkeit. Nicht Alarmmeldungen, sondern Entscheidungsfähigkeit. Nicht „Cyber", sondern Liquiditätsschutz, Vertragssicherheit, Ruhe im Management.

Rollenmodell in der Praxis: Gemeinsame Sicherheitsführung

Interne IT (Wertschöpfung)

- Hält den Betrieb stabil
- Kennt Geschäftsprozesse und Prioritäten
- Schafft Produktivitäts- und Wachstumsbeitrag

SYMPLASSON / Managed Security (Risikosteuerung)

- Überwacht sicherheitsrelevante Signale
- Priorisiert Meldungen und gibt klare Handlungspfade
- Testet und sichert Wiederherstellbarkeit
- Führt strukturiert in Stör-/Angriffsphasen
- Liefert Governance-, Nachweis- und Risikoreporting

> Das ist kein Outsourcing. Das ist Co-Steuerung digitaler Stabilität.

Die interne IT bleibt Dreh- und Angelpunkt der Wertschöpfung. SYM ergänzt systemische Fähigkeiten, die im Mittelstand schwer aufzubauen sind: Dauerbetrieb, Frühwarnung, Wiederherstellbarkeit, Transparenz, Führungsentlastung.

Key Insight

Mittelstand scheitert nie an fehlenden Tools. Er scheitert an fehlender Kapazität für Security-Betrieb.

Wirtschaftliche Leitfrage

„Wie teuer ist ein Jahr Unsicherheit im Vergleich zu einem Jahr Sicherheitsbetrieb?"

Ohne Managed Security

- Volatile Risiken
- Unklares Exposure
- Ungeplante Krisenkosten
- Management ohne Sichtbarkeit

Mit Managed Security

- Planbare OpEx
- Frühwarnsystem
- Wiederherstellbarkeit belegbar
- Transparenz für GF & Vorstand

Cyberresilienz ist längst kein IT-Budgetthema mehr, sondern ein Bestandteil moderner Unternehmensführung und Risikosteuerung. Unternehmen, die Führung heute zeitgemäß verstehen, betrachten Sicherheit als organisatorische Fähigkeit, Geschäftsmodelle unter digitalen Bedingungen stabil zu halten.

Das Ziel ist, nicht existenzbedrohlich getroffen werden zu können.

ROI-Modell: Sicherheitsbetrieb vs. Störkosten

Sicherheit amortisiert sich nicht durch Einsparung, sondern durch Störungskontrolle. Drei Mechanismen bestimmen den Return on Security Investment:

01

Vermeidung existenzbedrohender Vorfälle

→ Kapital- & Reputationsschutz

02

Verkürzung der Wiederanlaufzeit

→ Produktivitäts- & Umsatzsicherung

03

Freiwerdende interne Ressourcen

→ Fokus auf Wertschöpfung

Ein IT-Vorfall ohne Betriebsmodell kann aus Tagen Wochen machen – und aus Kostenfaktoren Liquiditätsrisiken. Mit geübter Wiederherstellung wird ein Vorfall zur Unterbrechung, nicht zum Desaster. Der ROI entsteht nicht, weil nichts passiert – sondern weil das, was passiert, keinen existentiellen Schaden mehr auslöst.

Business-Case-Matrix für den Mittelstand

Die folgende Matrix beleuchtet die finanziellen und operativen Auswirkungen einer Managed Security Lösung im Vergleich zu einem ungesicherten Betrieb für mittelständische Unternehmen:

Aspekt	Ohne Managed Security	Mit Managed Security
Risikomanagement	Hohe Angriffsfläche, unkalkulierbare Ausfallzeiten, Reputationsschaden.	Proaktive Abwehr, reduzierte Risikobereitschaft, schnelle Reaktion.
Kostenstruktur	Ungeplante Kosten für Incident Response und Datenwiederherstellung.	Planbare monatliche Betriebskosten (OpEx), Vermeidung hoher Einmalkosten.
Betriebliche Effizienz	Produktivitätsverlust durch Systemausfälle und manuelle Sicherheitsaufgaben.	Fokussierung der internen IT auf Kernaufgaben, minimierte Unterbrechungen.
Compliance & Governance	Gefahr von Strafen bei Nichteinhaltung von Vorschriften.	Unterstützung bei der Einhaltung relevanter Standards und Audits.

Managed Security verschiebt Risiko in Kosten — und damit in Steuerbarkeit. Das ist der eigentliche Business Case.

Governance statt Hoffnung

Security ohne Governance erzeugt falsche Ruhe. Security mit Governance erzeugt steuerbare Realität. Governance bedeutet hier die Übersetzung technischer Risiken in Führungs- und Steuergrößen:

Erkennungsgeschwindigkeit

Wie schnell erkennen wir Angriffe?

Wiederherstellungssicherheit

Wie sicher sind unsere Wiederanlaufprozeduren?

Kapazitätsbindung

Wie viel Kapazität binden wir in Störfällen?

Kritikalitätsbewertung

Welche Systeme haben höchste Kritikalität?

Testfrequenz

Wie regelmäßig testen wir Wiederherstellung?

Lieferkettensicherheit

Wie verlässlich sind Lieferketten?

Das Ziel ist nicht Perfektion, sondern Management-Fähigkeit. Unternehmen, die diese Fragen beantworten können, führen. Unternehmen ohne Antworten hoffen.

> Hoffnung ist keine Strategie und kein Schutz vor Haftungsrisiken.

SYMPLASSON-Modell: Sicherheitsbetrieb im Mittelstand

SYMPLASSON stellt Sicherheit nicht als Produkt bereit, sondern als betriebsfähige Funktion — vergleichbar mit einer Finanzcontrolling-Struktur, nur im digitalen Raum. Die interne IT bleibt Dreh- und Angelpunkt der Wertschöpfung. SYMPLASSON ergänzt dort, wo Mittelstand strukturell limitiert ist:

Dauerhafte Beobachtung

Kontinuierliche Überwachung sicherheitsrelevanter Signale

Priorisierung

Klare Handlungsempfehlungen und Eskalationspfade

Wiederherstellungstests

Regelmäßige Überprüfung von Backups und Recovery-Prozessen

Patch-Disziplin

Sicherstellung aktueller Systemstände

Ernstfall-Kommunikation

Strukturierte Eskalationsfähigkeit bei Vorfällen

Nachweisführung

Dokumentation für Geschäftsführung und Partner

SYMPLASSON liefert keine „Überwachung" — SYMPLASSON liefert digitale Handlungsfähigkeit.

Praxisfall: Der Unterschied zwischen Krise und Kontrolle

Ein anonymisierter Fall aus dem Mittelstand: Ein Mitarbeiter klickt auf einen präparierten Link. Zugangsdaten werden abgegriffen. Wenige Stunden später versuchen automatisierte Prozesse, internen Zugriff auszuweiten.

In einem reaktiven IT-Setup

Der Vorfall bleibt unbemerkt, bis Systeme ungewöhnliches Verhalten zeigen — oft zu spät, oft unbemerkt bis zum Stillstand.

- Keine Früherkennung
- Unkontrollierte Ausbreitung
- Produktionsausfall
- Existenzbedrohende Krise

Mit SYMPLASSON-Sicherheitsbetrieb

Die Aktivität wurde erkannt, gestoppt, Zugang entzogen, Backup-Integrität geprüft, Geschäftsleitung informiert — innerhalb eines Geschäftstages.

- Sofortige Erkennung
- Kontrollierte Reaktion
- Keine Betriebsunterbrechung
- Technisches Ereignis bleibt technisch

> **Ergebnis:** Der Vorfall blieb technisches Ereignis, nicht Unternehmenskrise. Und das Unternehmen verlor keine Stunde fakturierbarer Zeit.

Kennzahlen, die im Mittelstand wirklich zählen

Technische Metriken wie „Anzahl blockierter Angriffe" sind kosmetisch. Sie klingen beeindruckend, sagen aber wirtschaftlich wenig aus. Entscheider steuern nicht auf Firewallevents — sie steuern auf Funktion, Risiko und Zeit. Wirtschaftlich zählt nur Funktions- und Liquiditätssicherheit.

1. Zeitbasierte Kennzahlen

Wie lange bleibt das Unternehmen handlungsfähig?

KPI	Bedeutung	Wirtschaftliche Wirkung
MTTD – Mean Time to Detect	Zeit bis Erkennung	Bestimmt, wie tief ein Angriff eindringen kann
MTTR – Mean Time to Respond	Zeit bis Reaktion	Bestimmt, wie groß die Unterbrechung wird
RTO – Recovery Time Objective	Zulässige Wiederanlaufzeit	Bestimmt Produktions- & Lieferfähigkeit
RPO – Recovery Point Objective	Datenverlusttoleranz	Bestimmt Daten- & Umsatzverlust

Je schneller erkannt und reagiert wird, desto kürzer die Unterbrechung, desto geringer die Folgekosten. Das ist kein „Security-Vorteil". Das ist ein Cashflow-Puffer.

2. Verfügbarkeits-Kennzahlen

Welche Systeme dürfen niemals stillstehen?

Geschäftskritische IT

Umsatzmotor: ERP, CRM, DMS, Produktion

Kommunikation

Kundenzugang: Mail, Teams, Telefonie

Datenhaltung

Vertrags- & Know-how-Grundlage: Fileserver, Datenbanken

Identitäten

Zugang zur Arbeitsfähigkeit: Active Directory, Identity Provider

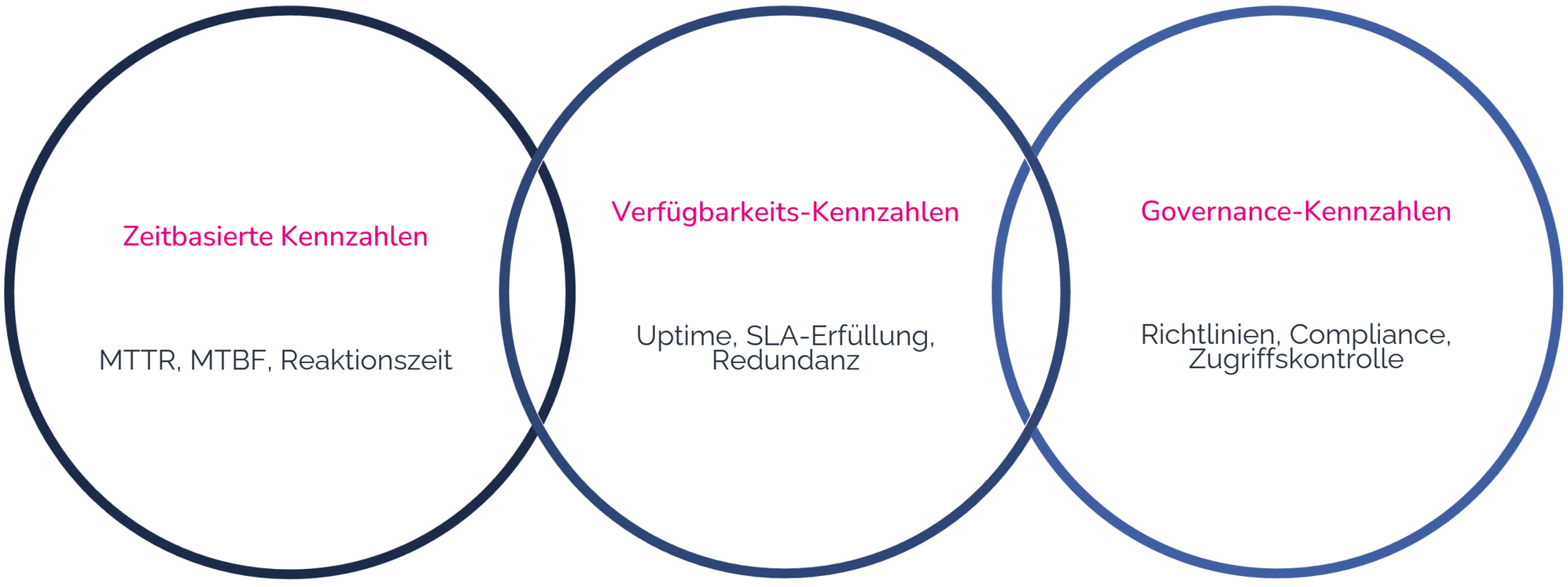
Der CFO braucht keine CVE-Liste – er braucht Klarheit, welche Prozesse bei Ausfall Umsatz stoppen.

3. Governance-Kennzahlen

Kann ich Sicherheit beweisen, nicht behaupten?

- **Patch-Compliance Rate:** Aktualitätsgrad kritischer Systeme
- **Backup-Restore-Erfolgsquote:** „Funktioniert Wiederherstellung oder hoffen wir nur?"
- **Audit-Trail / Reporting:** Nachweisfähigkeit für Geschäftsführung & Kunden
- **Incident-Response-Übungen:** Organisatorische Einsatzfähigkeit

> Was man nicht misst, kann man im Ernstfall nicht steuern.



Reifegradmodell und Handlungsschritte

Reife ist kein Reputationswort — sie ist Betriebsfähigkeit. Vier Stufen, klar definiert:

Stufe 1 — Reaktiv

Man vertraut Werkzeugen und glücklichen Umständen. Sicherheit ist Vermutung.

Schritt: Inventarisieren, Backup prüfen, Basis-Monitoring einführen.

Stufe 2 — Kontrolliert

Es gibt Prozesse — aber sie hängen an Personen, Priorität schwankt.

Schritt: Patch-Prozess hart definieren, Restore-Tests etablieren, Rollen trennen.

Stufe 3 — Proaktiv

Ereignisse werden erkannt, bewertet, bearbeitet. Reaktionsfähigkeit existiert.

Schritt: Reporting für Geschäftsführung, Incident-Playbooks, regelmäßige Tests.

Stufe 4 — Resilient

Sicherheit ist keine IT-Aufgabe, sondern Bestandteil der Unternehmenssteuerung.

Schritt: KPIs in Management-Rhythmus integrieren, Risiko wird gesteuert statt erlebt.

Ziel im Mittelstand: Stufe 3 mit klarer Bewegung auf Stufe 4.

Nicht Perfektion — Beherrschbarkeit.

Haftung & Compliance – der leise, harte Faktor

„IT macht das schon" ist kein juristisches Konzept.

Viele Geschäftsführer glauben, IT-Sicherheit sei delegierbar. Juristisch ist das falsch. Im deutschen Gesellschaftsrecht gilt: Die Geschäftsleitung bleibt verantwortlich für organisationale Vorkehrungen gegen vorhersehbare Risiken.

Das betrifft:

GmbH-Geschäftsführer

§ 43 GmbHG: Sorgfaltspflicht und Organisationsverantwortung

Vorstände

§ 93 AktG: Legalitätspflicht und Risikomanagement

Organisationspflichten

Nachweispflicht für systematische Risikosteuerung

DSGVO-Sorgfalt

Datenschutz als Führungsverantwortung

Das bedeutet nicht, dass Geschäftsführer Technik verstehen müssen. Es bedeutet: Sie müssen nachweisen können, dass Sicherheit systematisch geführt wird.

SYMPLASSON Managed Security liefert dafür:

- Dokumentierte Kontrollen
- Regelmäßige Berichte
- Prüf- und Testprotokolle
- Klare Zuständigkeiten
- Reaktionsfähigkeit

Damit wird aus „wir kümmern uns" ein haftungsfestes Organisationsprinzip.

Der wahre Wert: Stabilitätskultur

Unternehmen, die Sicherheit als Bestandteil von Planung, Reporting und Priorisierung verankern, erleben etwas, das in keiner Tool-Liste steht:

Ruhe.

Das Ergebnis strukturierter Sicherheit:

Weniger Ad-hoc-Entscheidungen

IT trifft planbare, strukturierte Entscheidungen

Lieferkettensicherheit

Sicherheit wird belegbar und kommunizierbar

Risikosichtbarkeit

Geschäftsführung sieht Risiken, statt sie zu erahnen

Wertschöpfungsfokus

Teams arbeiten an Wert statt an Bränden

Kundenvertrauen

Vertrauen steigt durch nachweisbare Stabilität

> Sicherheit schafft Management-qualität. Und Management-qualität schafft Wettbewerbsfähigkeit.

Fazit

Digitale Risiken verschwinden nicht. Aber sie lassen sich führen statt ertragen.

Managed Security verlagert Sicherheit dorthin, wo sie hingehört: in einen reproduzierbaren Betriebsprozess mit klarer Verantwortung, messbarer Wirkung und dokumentierter Belastbarkeit.

Reproduzierbare Prozesse Keine Improvisation, sondern erprobte Abläufe	**Klare Verantwortung** Definierte Rollen und Zuständigkeiten
Messbare Wirkung KPIs, die Führung ermöglichen	**Dokumentierte Belastbarkeit** Nachweisbare Resilienz für alle Stakeholder

Das ist der Unterschied zwischen Unternehmen, die auf Glück setzen, und Unternehmen, die auf Verlässlichkeit bauen.

> **Managed Security wandelt digitale Unsicherheit in betriebswirtschaftliche Verlässlichkeit um.**

Ein Mittelstandsunternehmen gewinnt nicht, weil es nie angegriffen wird. Es gewinnt, weil ein Angriff nicht zum Geschäftsereignis wird. Das ist kein Technikkauf. Das ist moderne Unternehmensführung im digitalen Zeitalter.

Bereit für mehr Sicherheit und Stabilität?

Sprechen Sie mit uns über Ihre digitale Sicherheitsstrategie und finden Sie heraus, wie Managed Security Ihr Unternehmen resilienter macht.

Kontakt

SYMPLASSON Informationstechnik GmbH

Holstenstraße 205

22765 Hamburg

Tel. +49 40 533 071-0

info@symplasson.de

www.symplasson.de

© 2025 — SYMPLASSON. Alle Rechte vorbehalten.

Hinweis: Dieses Dokument dient ausschließlich Informationszwecken und stellt keine Rechtsberatung dar. Alle Inhalte wurden sorgfältig erstellt, ersetzen jedoch keine individuelle Prüfung im Einzelfall. Angaben nach bestem Wissen, ohne Gewähr. Änderungen vorbehalten.