



DIGITALE RESILIENZ

In 90 Tagen zu mehr Sicherheit & Handlungsfähigkeit

Der Praxis-Guide für mittelständische Unternehmen



powered by



INHALT

Die neue Realität: Warum digitale Resilienz zur Managementaufgabe wird	3
Warum Sicherheit allein nicht reicht	4
Die neue Managementaufgabe	5
Sicherheit, Governance & Handlungsfähigkeit: Die 3 Fähigkeiten für den Unternehmenserfolg	7
Sicherheit beginnt mit Vertrauen auf Probe	8
Governance entsteht durch Transparenz	9
Handlungsfähigkeit im Notfall	10
Handlungsfähigkeit schafft Vertrauen	11
Der Einsatz von Technologien für Sicherheit, Kontrolle und Handlungsfähigkeit	12
Wie Microsoft die 3 Fähigkeiten unterstützt	13
Vom Know-how zum Do-how: Der 90-Tage-Plan	15
Phase 1: Transparenz schaffen	16
Phase 2: Governance stärken	17
Phase 3: Handlungsfähigkeit testen	18
Fazit: Chancen nutzen & Risiken beherrschen	19



DIE NEUE REALITÄT

WARUM DIGITALE RESILIENZ ZUR MANAGEMENTAUFGABE WIRD

Im Sommer 2026 sorgte ein Cyberangriff auf die Berliner Verwaltung bundesweit für Schlagzeilen. Über Wochen hinweg konnten Angreifer durch fehlende Multifaktor-Authentifizierung und sorglos in Word-Dateien gespeicherte Zugangsdaten unbemerkt eindringen und große Datenmengen kopieren. Nachdem die geforderte Lösegeldsumme von 2 Mio. EUR nicht gezahlt wurde, veröffentlichten die Täter Millionen von Dateien im Darknet, darunter sensible Verwaltungs- und Infrastrukturdaten. Der Vorfall machte deutlich, wie weitreichend die Folgen sein können, wenn Informationen plötzlich außerhalb der eigenen Kontrolle geraten.

Gleichzeitig ist der wirtschaftliche Schaden durch Cyberkriminalität in den letzten Jahren kontinuierlich angestiegen. Laut [Bitkom](#) verursachten Cyberangriffe im Jahr 2025 Schäden von rund 202 Milliarden Euro in der deutschen Wirtschaft. Zusammen mit Datendiebstahl, Industriespionage und Sabotage belief sich der Gesamtschaden sogar auf rund 289 Milliarden Euro. Für 2026 wird zwar ein leichter Rückgang prognostiziert, das Niveau bleibt jedoch bei weit über 200 Milliarden EUR.

Doch Cyberkriminalität ist längst nicht mehr die einzige Herausforderung. Mit dem inzwischen geltenden NIS2-Gesetz sind Cybersicherheit, Risikomanagement und klare Verantwortlichkeiten zur Managementaufgabe geworden. Doch mit der Umsetzung tun sich viele Unternehmen schwer. Die Anforderungen erscheinen komplex, die Ressourcen sind begrenzt und im Tagesgeschäft fehlt oft die Zeit, sich strukturiert mit Risiken, Daten, Berechtigungen und Notfallszenarien auseinanderzusetzen. Vertreter der Wirtschaft weisen deshalb seit längerem darauf hin, dass insbesondere mittelständische Unternehmen praktikable und verständliche Ansätze benötigen, um die gesetzlichen und wirtschaftlichen Anforderungen bewältigen zu können.

Gleichzeitig treiben Digitalisierung und Künstliche Intelligenz die Entwicklung weiter voran. Informationen entstehen heute in Cloud-Plattformen, werden in E-Mails, Teams-Chats und Geschäftsanwendungen verarbeitet und zunehmend auch von KI-Systemen genutzt. Das eröffnet enorme Chancen für

1. **Wer darf auf welche Informationen zugreifen?**
2. **Was passiert, wenn ein kritisches System plötzlich nicht mehr verfügbar ist?**
3. **Welche Daten werden durch KI verarbeitet?**
4. **Welche Abhängigkeiten bestehen innerhalb des Ökosystems des eigenen Unternehmens?**

Viele Unternehmen suchen auf diese Fragen vor allem technische Antworten. Tatsächlich geht es jedoch um weit mehr als Technologie. Es geht darum, die eigene digitale Umgebung bewusst zu gestalten, Risiken zu steuern und auch in schwierigen Situationen handlungsfähig zu bleiben.

Genau dabei unterstützt Sie dieses Whitepaper. Es zeigt, warum digitale Resilienz heute auf drei Fähigkeiten basiert: **Sicherheit, Governance und Handlungsfähigkeit.**

Denn Unternehmen, die ihre digitalen Risiken verstehen, klare Spielregeln etablieren und sich auf kritische Situationen vorbereiten, schaffen die Grundlage für einen sicheren, verantwortungsvoll gesteuerten und widerstandsfähigen Geschäftsbetrieb. Und genau den Weg dorthin zeigen wir Ihnen mit unserem 90-Tage-Plan auf den folgenden Seiten.





WARUM SICHERHEIT ALLEIN NICHT REICHT

Lange Zeit lautete die zentrale Frage vieler Unternehmen: Wie schützen wir uns vor Cyberangriffen?

Diese Frage ist nach wie vor wichtig, nur greift sie heute viel zu kurz. Denn selbst die beste Sicherheitslösung kann nicht jede Bedrohung verhindern. Cyberkriminelle werden täglich professioneller und ihre Angriffe gezielter. Gleichzeitig werden die digitalen Landschaften in Unternehmen komplexer und täglich entstehen neue Daten, Anwendungen und KI-gestützte Prozesse.

Ein aktuelles Beispiel zeigt, wie wenig moralische Grenzen Cyberkriminelle inzwischen kennen. Selbst die Welthungerhilfe, die weltweit Menschen in Not unterstützt, wurde Ziel eines Cyberangriffs. Die selbe Angreifergruppe, die auch die Berliner Verwaltung attackierten, forderten 1,8 Mio. Euro Lösegeld und veröffentlichten Daten im Darknet.

Der Vorfall macht deutlich: Weder Branche noch Unternehmensgröße oder gesellschaftlicher Auftrag schützen vor digitalen Risiken. Das BKA verdeutlicht im jüngst veröffentlichten [Bundeslagebild Cybercrime](#), dass 90% der Angriffe auf kleine und mittelständische Unternehmen gerichtet sind. Eben weil der Mittelstand immer noch zu wenig in Sicherheit, Governance und Handlungsfähigkeit investiert und damit ein leichtes Ziel ist.

Die entscheidende Frage lautet deshalb nicht mehr allein: Wie verhindern wir erfolgreich einen Angriff, sondern vielmehr: Wie gut kennen wir unsere kritischen Informationen, Risiken und Abhängigkeiten und wie handlungsfähig bleiben wir, wenn trotz aller Vorsichtsmaßnahmen etwas passiert?

Gerade durch Cloud-Plattformen, mobiles Arbeiten und Künstliche Intelligenz entstehen neue Herausforderungen. Informationen werden an vielen Orten gespeichert, von unterschiedlichen Anwendungen verarbeitet und von immer mehr Personen, Partnern und Systemen genutzt.

Dadurch rücken zusätzliche Fragestellungen in den Mittelpunkt:

- **Welche Daten** benötigen welchen **Schutz**?
- **Welche Prozesse** sind **geschäftskritisch**?
- **Welche Risiken** akzeptieren wir **bewusst**?
- **Welche Abhängigkeiten** sind für uns **vertretbar**?
- **Wo** benötigen wir **zusätzliche Sicherheits- und Steuerungsmechanismen**?





DIE NEUE MANAGEMENTAUFGABE

Auf den vorherigen Seiten haben wir gesehen, dass Unternehmen heute mit deutlich mehr Herausforderungen konfrontiert sind als noch vor wenigen Jahren. Cyberangriffe, regulatorische Anforderungen wie NIS2, Cloud-Plattformen, hybride Arbeitsmodelle und Künstliche Intelligenz verändern die Art und Weise, wie Informationen verarbeitet und Geschäftsprozesse gesteuert werden.

Deshalb reicht es nicht mehr aus, Sicherheit ausschließlich als IT-Thema zu betrachten. Denn die entscheidenden Fragen sind heute nicht mehr rein technisch zu beantworten, wie wir auf der vorhergehenden Seite gesehen haben.

Die Antworten auf die Frage „Wie bleiben wir arbeits- und lieferfähig, wenn ein wichtiger Service ausfällt?“ können nicht allein von der IT-Abteilung gegeben werden. Sie betreffen die gesamte Organisation und müssen auf Managementebene getroffen werden.

Dabei geht es ausdrücklich nicht darum, jede Aktivität zu kontrollieren oder jedes Risiko auszuschließen, da es weder realistisch noch wirtschaftlich sinnvoll wäre. Entscheidend ist vielmehr, die richtigen Leitplanken zu setzen, geeignete Maßnahmen sowie Verantwortlichkeiten zu definieren und dort Transparenz zu schaffen, wo sie für das Unternehmen wirklich notwendig ist.

Genau das verstehen wir unter Governance.

Bedeutung von Governance im IT-Kontext:

Governance bedeutet nicht Überwachung. Governance bedeutet, klare Spielregeln für den Umgang mit Daten, Risiken, Zugriffsrechten und Verantwortlichkeiten zu schaffen.

Sie sorgt dafür, dass Unternehmen wissen, welche Informationen besonders schützenswert sind, wer Entscheidungen treffen darf, welche Risiken bewusst akzeptiert werden und welche Maßnahmen im Ernstfall greifen.

Kurz gesagt: Governance schafft Orientierung, Transparenz und Verlässlichkeit.



Unternehmen, die diese Spielregeln etablieren, schaffen die Grundlage für fundierte Entscheidungen, wirksame Sicherheitsmaßnahmen und einen professionellen Umgang mit unerwarteten Ereignissen.

Genau so entsteht digitale Resilienz. Sie basiert auf drei Fähigkeiten, die sich gegenseitig ergänzen:

- **Sicherheit schützt vor Bedrohungen und reduziert Risiken.**
- **Governance schafft Transparenz, Verantwortlichkeiten und klare Leitplanken.**
- **Handlungsfähigkeit sorgt dafür, dass das Unternehmen auch in kritischen Situationen arbeitsfähig bleibt.**

Gemeinsam bilden diese drei Fähigkeiten das Fundament für einen sicheren, verantwortungsvoll gesteuerten und zukunftsfähigen Geschäftsbetrieb.

Von IT-Sicherheit zu digitaler Resilienz

FRÜHER

Systeme schützen

Der Schutz konzentrierte sich vor allem auf die technische Umgebung und wurde von der IT gewährleistet

- 1 **Firewall** Netzwerkgrenzen absichern
- 2 **Virenschutz** Schadsoftware erkennen
- 3 **Backup** Daten wiederherstellen
- 4 **Netzwerk** Zugänge kontrollieren

Digitalisierung
Cloud
Vernetzung
KI



HEUTE

Das digitale Unternehmen ganzheitlich steuern

Digitale Resilienz umfasst heute das gesamte Zusammenspiel von:

Daten

Menschen

Geräte

Apps

Cloud

KI

Dritte

Prozesse

Die Managementaufgabe:

Zusammenhänge verstehen, klare Spielregeln schaffen und Risiken sowie Abhängigkeiten bewusst steuern.





SICHERHEIT, GOVERNANCE & HANDLUNGSFÄHIGKEIT

DIE 3 FÄHIGKEITEN FÜR DEN UNTERNEHMENSERFOLG

Jedes Unternehmen verfügt heute über einen digitalen Maschinenraum. ERP- und CRM-Systeme steuern Vertriebsprozesse, Auftragsabwicklung, Logistik und Finanzen. Hinzu kommen Kundenportale, Cloud-Dienste sowie zunehmend auch Künstliche Intelligenz, die bei Recherche, Kommunikation und ersten Geschäftsprozessen unterstützt.

Auch wenn sich viele Unternehmen noch nicht als besonders digital bezeichnen, können wir uns ohne IT und digitales Arbeiten den Arbeitsalltag gar nicht mehr vorstellen. Bewusst wird das den meisten erst, wenn eines der wichtigen Systeme ausfällt. Bereits eine halbe Stunde Stillstand zeigt die Auswirkungen, die vor wenigen Jahren noch undenkbar gewesen wären.

Deshalb stellt sich für die Geschäftsführung eine zentrale Frage:

Wie gut ist unser Unternehmen darauf vorbereitet, die Chancen der Digitalisierung sicher zu nutzen, klare Spielregeln für Daten und Risiken zu etablieren und auch in schwierigen Situationen handlungsfähig zu bleiben?

Sicherheit, Governance & Handlungsfähigkeit

Die drei Fähigkeiten für einen verlässlichen Geschäftsbetrieb



Erst das Zusammenspiel der drei Fähigkeiten schafft die Grundlage für einen stabilen und zukunftsfähigen Geschäftsbetrieb.





SICHERHEIT BEGINNT MIT VERTRAUEN AUF PROBE

In vielen Unternehmen galt lange Zeit ein einfaches Prinzip: Wer im Unternehmensnetzwerk arbeitet, dem wird vertraut. Die heutige moderne Arbeitswelt funktioniert jedoch anders. Mitarbeitende arbeiten aus dem Homeoffice, greifen im Außendienst von unterwegs auf Daten zu und nutzen unterschiedlichste Anwendungen in der Cloud. Hinzu kommen externe Dienstleister und zunehmend auch KI-Agenten, die selbstständig Informationen verarbeiten oder Prozesse autonom steuern.

Deshalb basiert moderne Sicherheit heute auf einem anderen Grundsatz: Vertraue niemandem, prüfe jede Anfrage. Genau dieser Gedanke steckt hinter dem Zero-Trust-Ansatz. Dabei spielt es keine Rolle, ob es sich um einen Mitarbeitenden, einen Dienstleister, eine Anwendung oder einen KI-Agenten handelt. Jeder Zugriff wird anhand klarer Kriterien bewertet:

- **Wer** möchte zugreifen?
- **Von welchem Gerät** erfolgt der Zugriff?
- **Welche Informationen** werden benötigt bzw. angefragt?
- Ist die Anfrage **plausibel**?
- Besteht ein **erhöhtes Risiko**?

Das Ziel ist nicht Misstrauen gegenüber Mitarbeitenden, sondern Risiken frühzeitig zu erkennen und Angreifern möglichst wenig Angriffsfläche zu bieten. Der Zero-Trust-Ansatz hilft dabei, dass jeder Zugriff explizit und nachvollziehbar geprüft wird.

Darüber hinaus regelt er, dass nur Rechte vergeben werden, die tatsächlich benötigt werden. Nicht jeder Mitarbeitende benötigt Zugriff auf sämtliche Informationen, gleiches gilt für Anwendungen und KI-Systeme. Je gezielter Berechtigungen vergeben werden, desto geringer wird das Risiko eines Missbrauchs.

Was bedeutet das für Sie im Unternehmen? Es ist nicht die Anzahl der Sicherheitswerkzeuge, die über die Sicherheit eines Unternehmens entscheidet. **Vielmehr ist es die Fähigkeit, Zugriffe nachvollziehbar zu steuern, Risiken frühzeitig zu erkennen, Berechtigungen regelmäßig zu überprüfen und Schäden wirksam zu begrenzen.**





GOVERNANCE ENTSTEHT DURCH TRANSPARENZ

Mit IT- und Cybersicherheit beantworten wir die Frage, wie wir unser Unternehmen vor Angriffen von innen und außen bestmöglich schützen. Governance beantwortet hingegen eine andere Frage: Wissen wir eigentlich, welche Informationen, Risiken und Abhängigkeiten in unserem Unternehmen bestehen und wie wir damit umgehen?

Jetzt werden Sie sich sicherlich denken: „Natürlich weiß ich, was in meinem Unternehmen passiert, was für eine Frage!“ Ganz so einfach ist es aus unserer Erfahrung leider nicht. Insbesondere in über Jahre gewachsenen IT- und Datenlandschaften fällt es vielen Unternehmen schwer, einen vollständigen Überblick über Informationen, Berechtigungen, KI-Nutzung und externe Abhängigkeiten zu gewinnen.

Folgende Fragen sollten deshalb klar beantwortet werden können:

- **Welche sensiblen Daten** sind vorhanden und welche sind noch wichtig?
- **Wo** überall sind Daten gespeichert?
- **Wer** kann darauf zugreifen?
- **Welche Daten** dürfen von **KI-Systemen verwendet** werden und **welche werden tatsächlich verwendet**?
- **Welche Dienstleister bzw. GeschäftspartnerInnen** sind eingebunden?
- **Welche Abhängigkeiten bestehen** von Plattformen und Herstellern?

Genau hier setzt die zweite wichtige Fähigkeit moderner Unternehmen an: Governance.

Governance bedeutet nicht Bürokratie oder Überwachung. Governance bedeutet, klare Spielregeln für Daten, Zugriffe, Risiken und Verantwortlichkeiten zu schaffen.

Dafür braucht es vor allem Transparenz. Unternehmen müssen nachvollziehen können, welche Informationen vorhanden sind, wer darauf zugreifen darf, welche Anwendungen diese Informationen nutzen und welche Risiken daraus entstehen können. Klare Rollen, Verantwortlichkeiten und Berechtigungen sorgen dafür, dass Informationen dort verfügbar sind, wo sie benötigt werden, und gleichzeitig wirksam geschützt bleiben. Darüber hinaus sollte regelmäßig Datenhygiene betrieben werden, damit Daten nur so lange gespeichert sind, wie sie im Unternehmen tatsächlich benötigt werden.

Gleichzeitig müssen Unternehmen ihre digitalen Abhängigkeiten bewusst steuern. Cloud-Dienste, externe Dienstleister und KI-Plattformen gehören heute zum Geschäftsalltag. Governance bedeutet deshalb auch, Risiken regelmäßig zu bewerten, Verantwortlichkeiten festzulegen und bei kritischen Prozessen Alternativen zu kennen.

Wer diese Transparenz besitzt, kann fundierte Entscheidungen treffen, Risiken besser steuern und den Einsatz neuer Technologien wie Künstlicher Intelligenz verantwortungsvoll gestalten.



HANDLUNGSFÄHIGKEIT IM NOTFALL

Kein Unternehmen plant einen Cyberangriff, einen längeren Strom- bzw. Systemausfall oder eine Naturkatastrophe. Allerdings gehören solche Situationen inzwischen zur Realität. Die entscheidende Frage ist deshalb nicht, ob Störungen auftreten können, sondern: **Wie gut ist Ihr Unternehmen darauf vorbereitet?**

Viele größere Unternehmen investieren erhebliche Summen in den Schutz ihrer Systeme, was auch sehr wichtig ist. Gleichzeitig zeigt die Praxis, dass selbst die besten Sicherheitsmaßnahmen keinen hundertprozentigen Schutz bieten können.

Handlungsfähigkeit beginnt daher dort, wo Sicherheit an ihre Grenzen stößt. Sie beschreibt die Fähigkeit eines Unternehmens, auch unter schwierigen Bedingungen arbeitsfähig, lieferfähig und entscheidungsfähig zu bleiben.

Am einfachsten und häufigsten passieren Systemausfälle. Sie kennen das sicherlich: Das ERP-System steht, Aufträge können nicht bearbeitet werden, ohne Lieferscheine keine Auslieferung und die Kommunikationsdrähte laufen heiß, weil GeschäftspartnerInnen auf Rückmeldungen warten.

In diesem Moment interessiert niemanden mehr, welche Technologie eingesetzt wird oder wie modern die Sicherheitslösung ist. Entscheidend ist nur noch: Wissen wir, was jetzt zu tun ist?

Handlungsfähigkeit beginnt lange vor dem Notfall

Unternehmen, die Krisen gut bewältigen, unterscheiden sich häufig nicht durch mehr Technologie. Sie unterscheiden sich durch bessere Vorbereitung.

Sie wissen beispielsweise:

- welche Prozesse für das Unternehmen unverzichtbar sind,
- welche Systeme zuerst wieder verfügbar sein müssen,
- welche Daten besonders kritisch sind,
- wer Entscheidungen treffen darf,
- wie intern und extern kommuniziert wird,
- und welche Alternativen im Ernstfall zur Verfügung stehen.

Diese Klarheit spart im Notfall wertvolle Zeit.





HANDLUNGSFÄHIGKEIT SCHAFFT VERTRAUEN

Besonders in mittelständischen Unternehmen hängt viel Wissen von einzelnen Personen ab: Der IT-Leiter kennt die Systemlandschaft, die Produktionsleitung weiß, welche Aufträge Priorität haben, der Vertrieb kennt die wichtigsten Kunden und die Buchhaltung kümmert sich um Zahlungsverkehr und Gehaltsabrechnung.

Doch was passiert, wenn genau diese Personen nicht erreichbar sind?

Handlungsfähigkeit bedeutet deshalb auch, Verantwortung klar zu regeln und Wissen nicht ausschließlich bei einzelnen Mitarbeitenden zu konzentrieren. Wer darf Systeme abschalten? Wer informiert Kunden? Wer entscheidet über Prioritäten? Wer spricht mit Dienstleistern oder Behörden? Je klarer diese Fragen beantwortet sind, desto ruhiger und strukturierter kann ein Unternehmen reagieren.

Ganz wichtig dabei ist: Handlungsfähigkeit bedeutet nicht Perfektion! Viele Unternehmen glauben, sie müssten für jedes denkbare Szenario einen ausgearbeiteten Notfallplan vorhalten, doch in der Praxis ist der Weg das Ziel. Sprich es müssen für die wichtigsten Szenarien gut ausgearbeitete und regelmäßig aktualisierte Notfallpläne vorhanden sein.

- **Welche drei Prozesse** würden Ihr Unternehmen am **schnellsten zum Stillstand bringen**?
- **Welche Systeme** müssen innerhalb weniger Stunden **wieder verfügbar sein**?
- **Welche Informationen** werden benötigt, um den **Geschäftsbetrieb aufrechtzuerhalten**?
- **Welche Arbeiten** könnten vorübergehend auch **auf andere Weise erledigt werden**?

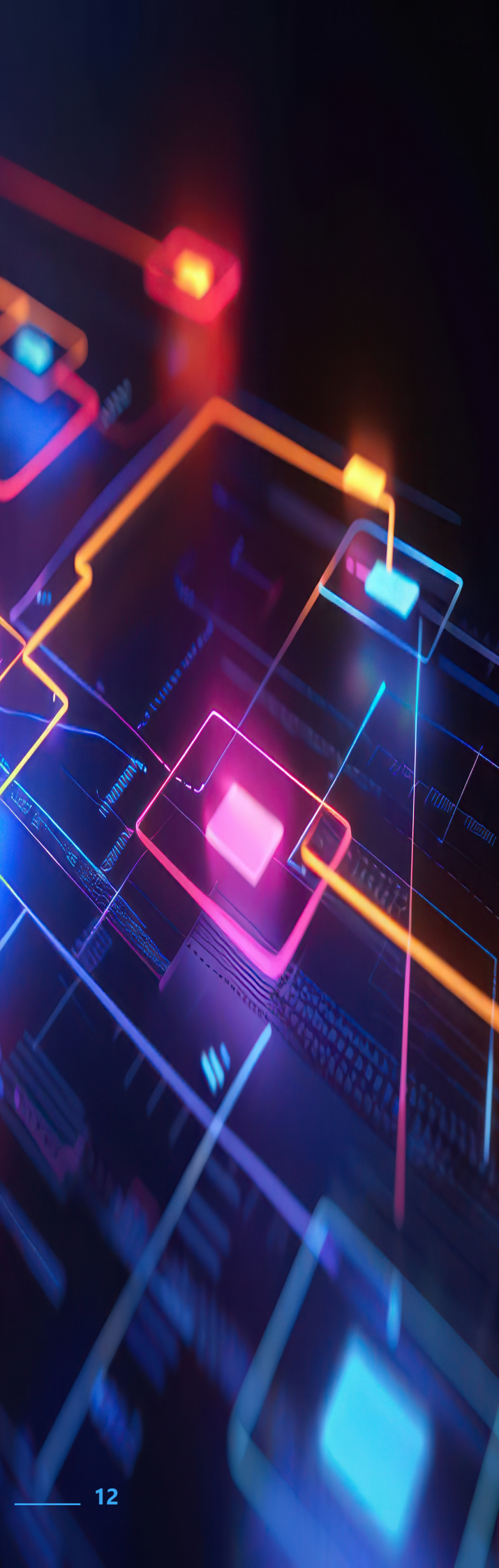
Oft reichen bereits wenige, gut vorbereitete Maßnahmen aus, um die Auswirkungen eines Vorfalls erheblich zu reduzieren. Zudem erwarten Kunden, Lieferanten und Mitarbeitende heute nicht, dass niemals Probleme auftreten. Was sie aber schon erwarten, ist ein professioneller Umgang mit Notfallsituationen.

Mindestens ebenso wichtig ist, dass jeder Mitarbeitende weiß, wo diese Notfallpläne abgerufen werden können - sonst nützen im Fall der Fälle die besten Pläne nichts.

Abgesehen davon wird ein Betrieb, der auch unter schwierigen Bedingungen verlässlich liefert, kommuniziert und Entscheidungen trifft, als stabiler und vertrauenswürdiger Geschäftspartner wahrgenommen.

Genau deshalb ist Handlungsfähigkeit weit mehr als ein IT-Thema. Sie ist ein wesentlicher Bestandteil moderner Unternehmensführung.





DER EINSATZ VON TECHNOLOGIEN FÜR SICHERHEIT, GOVERNANCE UND HANDLUNGSFÄHIGKEIT

Auf den letzten Seiten ist klar geworden, dass Technologie allein all die Herausforderungen nicht lösen kann.

Die entscheidende Grundlage bilden klare Verantwortlichkeiten, nachvollziehbare Prozesse und ein gemeinsames Verständnis darüber, welche Informationen, Systeme und Geschäftsprozesse besonders schützenswert sind.

Was moderne Plattformen wie Microsoft jedoch sehr gut können, ist Unternehmen dabei zu unterstützen, diese Anforderungen deutlich einfacher umzusetzen.

Gerade mittelständische Unternehmen stehen häufig vor einer besonderen Herausforderung: Sie müssen ein hohes Sicherheitsniveau erreichen, verfügen aber selten über große interne Spezialistenteams. Hier spielen integrierte Cloud- und Sicherheitsplattformen ihre Stärken aus. Sie helfen dabei, Informationen zu schützen, Zugriffe zu steuern, Bedrohungen frühzeitig zu erkennen und den Geschäftsbetrieb auch in schwierigen Situationen aufrechtzuerhalten.

Microsoft verfolgt dabei einen ganzheitlichen Ansatz, der auf den Prinzipien von Zero Trust basiert. Zugriffe werden kontinuierlich geprüft, Berechtigungen auf das notwendige Maß beschränkt und potenzielle Sicherheitsvorfälle von Anfang an berücksichtigt.

Die gute Nachricht ist: Die meisten Unternehmen haben durch Microsoft 365 ab den Versionen Business Premium und höher bereits eine solide Basis an Diensten zur Verfügung. Oftmals fehlt es allerdings an Know-how und Zeit, die enthaltenen Möglichkeiten zielgerichtet auszuschöpfen.

Auf den folgenden Seiten zeigen wir Ihnen, wie Microsoft die einzelnen Säulen Sicherheit, Governance und Handlungsfähigkeit unterstützt.

Das Beste kommt wie immer zum Schluss: Wir zeigen Ihnen, wie Sie mit welchen Schritten innerhalb von 90 Tagen die drei Säulen im Unternehmen stärken können.



WIE MICROSOFT DIE DREI FÄHIGKEITEN UNTERSTÜTZT

SICHERHEIT

Mit den umfangreichen Microsoft 365 Business-Premium Lizenzen haben Sie schon eine hervorragende Basis, sie muss nur entsprechend konfiguriert und implementiert werden.

Dazu gehören beispielsweise:

- Schutz von Benutzerkonten und Anmeldungen
- Sicherheitsrichtlinien für Endgeräte
- Schutz vor Phishing, Malware und Ransomware
- Überwachung sicherheitsrelevanter Ereignisse
- Unterstützung durch KI-gestützte Bedrohungsanalyse
- Erkennung und Eindämmung von Sicherheitsvorfällen
- Schutz sensibler Unternehmensdaten über Anwendungen und Geräte hinweg

Der Zero-Trust-Ansatz von Microsoft verfolgt dabei das Ziel, Risiken frühzeitig zu erkennen, Angriffsflächen zu reduzieren und mögliche Schäden wirksam zu begrenzen. So entsteht eine Sicherheitsbasis, auf der moderne Zusammenarbeit, Cloud-Nutzung und Künstliche Intelligenz verantwortungsvoll genutzt werden können.

GOVERNANCE

Der Schutz von Daten und insbesondere von sensiblen Informationen ist heute nicht nur für die Cybersicherheit entscheidend, sondern auch für den verantwortungsvollen Einsatz von Künstlicher Intelligenz. Microsoft unterstützt Unternehmen dabei,

- Daten zu klassifizieren,
- Zugriffe nachvollziehbar zu steuern,
- Berechtigungen zu verwalten,
- Information Governance umzusetzen,
- den Einsatz von KI verantwortungsvoll zu gestalten.

Besonders für den Einsatz von Microsoft Copilot ebenso wie individuelle KI-Agenten und Workflows gewinnt diese Transparenz an Bedeutung.

Darüber hinaus bietet Microsoft zusätzliche Funktionen an, die Unternehmen mehr Transparenz und Steuerungsmöglichkeiten für Datenhaltung, Verschlüsselung, Zugriffe und Betriebsprozesse ermöglichen. Dazu gehören beispielsweise kundenkontrollierte Schlüssel, europäische Datenhaltung und erweiterte Governance- und Verwaltungsfunktionen für Cloud-Umgebungen.

KI zeigt keine geheimen Daten - sie bringt Versäumnisse ans Licht

Den größten Mehrwert bringen KI-Modelle wie Microsoft Copilot, wenn sie auf Unternehmensdaten zugreifen. Wenn Sie Ihre Daten & Berechtigungen nicht in Ordnung gebracht haben, **wirkt Copilot wie ein Scheinwerfer auf Ihre digitale Arbeitsumgebung.**

Er erzeugt keine Berechtigungslücken, **sondern macht sichtbar, wo Datenablagen, Zugriffsrechte oder Governance bisher nicht konsequent umgesetzt wurden.**



HANDLUNGSFÄHIGKEIT

Wir wissen heute alle: Ohne IT läuft selbst in Handwerksbetrieben kaum noch ein Prozess. Deshalb ist die Absicherung der Arbeitsfähigkeit ein wichtiger Teil von Notfallplänen. Microsoft unterstützt die Wiederherstellung der IT-Systeme unter anderem durch:

- Cloud-basierte Backup- und Wiederherstellungsmöglichkeiten
- hochverfügbare Cloud-Dienste
- integrierte Sicherheits- und Monitoringlösungen
- Business-Continuity-Konzepte
- unterschiedliche Betriebsmodelle bis hin zu hybriden und lokalen Szenarien

Darüber hinaus unterstützen wir Sie mit unseren Managed Service Angeboten darin, alle drei Säulen bestmöglich abzusichern und im Notfall schnellstmöglich wieder arbeitsfähig zu sein.

Microsoft-Technologien als Wegbereiter

Eine gemeinsame Plattform unterstützt Unternehmen dabei, Sicherheit, Governance und Handlungsfähigkeit im Alltag zu verankern.





VOM KNOW-HOW ZUM DO-HOW: DER 90-TAGE-PLAN

Keine Frage: Viele Unternehmen wissen nur zu gut, dass sie sich mit Sicherheit, Governance und Handlungsfähigkeit beschäftigen müssen. Die eigentliche Herausforderung besteht wie so oft darin, aus guten Vorsätzen konkrete Maßnahmen abzuleiten.

Die gute Nachricht lautet: Niemand muss alles auf einmal erledigen. Unsere Teams begleiten Sie auf dem Weg zu Ihrem individuellen Ziel an Sicherheit, Governance und Handlungsfähigkeit.

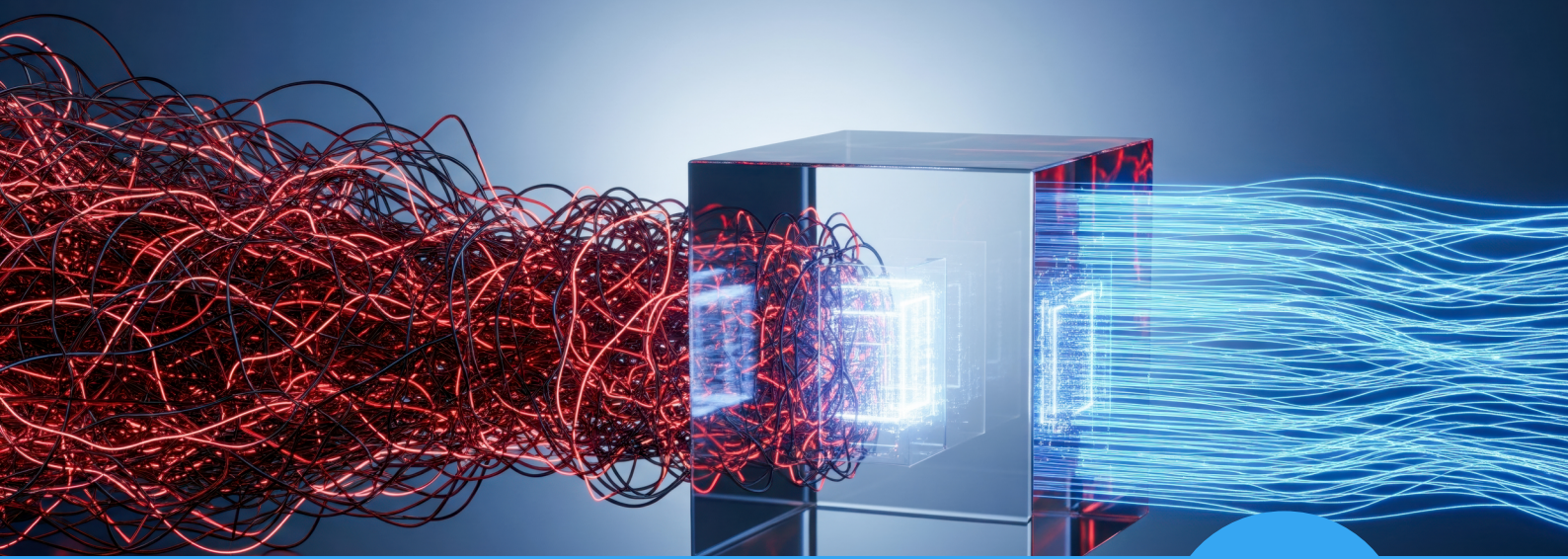
Aus unserer Erfahrung und mit unserem Improvement-Modell können wir Ihnen heute versichern, dass bereits wenige gut gewählte Schritte innerhalb kurzer Zeit für mehr Transparenz, bessere Entscheidungen und deutlich weniger Risiken sorgen können - ganz nach unserem Leitspruch:
„run your business smarter“

Der folgende 90-Tage-Plan zeigt einen pragmatischen, mittelstandsgerechten Einstieg:

In 90 Tagen vom Wissen ins Handeln

Ein pragmatischer Einstieg für mehr Sicherheit, Governance und Handlungsfähigkeit





Tag
1-30

PHASE 1: TRANSPARENZ SCHAFFEN

Die ersten vier Wochen dienen einem elementaren Ziel: Verstehen, wo das Unternehmen heute steht.

Bevor neue Richtlinien eingeführt, Technologien beschafft oder Projekte gestartet werden, sollte zunächst Klarheit darüber geschaffen werden, welche Informationen, Systeme und Prozesse für den Geschäftsbetrieb wirklich wichtig sind. Viele Unternehmen sind überrascht, welche Erkenntnisse bereits eine einfache Bestandsaufnahme liefert.

Oft stellt sich heraus, dass sensible Daten an unerwarteten Orten gespeichert werden, Berechtigungen über Jahre gewachsen sind oder niemand genau sagen kann, welche Anwendungen im Arbeitsalltag tatsächlich genutzt werden. Typische Fragen dieser Phase sind:

- Welche Prozesse sind für Umsatz, Produktion und Lieferfähigkeit unverzichtbar?
- Welche Daten wären besonders kritisch, wenn sie veröffentlicht würden?
- Welche Security-, Cloud-Dienste und KI-Anwendungen werden tatsächlich genutzt?
- Welche Dienstleister besitzen Zugriff auf Unternehmensdaten?
- Wo bestehen größere Abhängigkeiten von einzelnen Personen, Plattformen oder Anwendungen?

Die gute Nachricht in dieser Phase ist: Einige Risiken lassen sich bereits in den ersten Tagen mit wenigen, pragmatischen Maßnahmen spürbar reduzieren. Typische Quick Wins sind:

- **Multifaktor-Authentifizierung** für alle Benutzerkonten aktivieren
- Nicht mehr benötigte **Benutzerkonten und Berechtigungen bereinigen**
- **Wichtige Notfallkontakte** und **Verantwortlichkeiten** dokumentieren
- Gemeinsamen **Speicherort** für **Notfallpläne und Dokumentationen** festlegen

Das Ergebnis nach 30 Tagen:

Sie wissen, welche Bereiche Ihres Unternehmens bei einem Cyberangriff oder Systemausfall zuerst betroffen sein können. Kritische Prozesse, sensible Informationen, externe Abhängigkeiten und die wichtigsten Risiken sind transparent und priorisiert.

Gleichzeitig wurden bereits erste Sofortmaßnahmen umgesetzt: Benutzerkonten wurden zusätzlich abgesichert, Notfallkontakte dokumentiert und erste organisatorische Schwachstellen beseitigt. Aus vielen Einzelinformationen entsteht erstmals ein gemeinsames Verständnis darüber, wo Handlungsbedarf besteht und welche Maßnahmen den größten Nutzen für Ihr Unternehmen bringen.





Tag
31-60

PHASE 2: GOVERNANCE STÄRKEN

Nachdem Transparenz geschaffen wurde, geht es in der zweiten Phase darum, Ordnung und klare Spielregeln einzuführen.

Viele Risiken entstehen nicht durch fehlende Technologie, sondern durch gewachsene Strukturen. Mitarbeitende besitzen Berechtigungen, die sie längst nicht mehr benötigen, Daten werden mehrfach gespeichert und neue KI-Werkzeuge werden genutzt, ohne dass klare Regeln festgelegt wurden. In dieser Phase werden deshalb die wichtigsten Leitplanken definiert.

Typische Maßnahmen sind:

- Überprüfung von Benutzerkonten und Berechtigungen
- Optimierung der Mehrfaktor-Authentifizierung
- Klassifizierung besonders sensibler Informationen
- Definition von Regeln für Cloud- und KI-Nutzung
- Benennung von Verantwortlichkeiten für geschäftskritische Daten und Systeme
- Dokumentation wichtiger Dienstleister und externer Zugriffe

In dieser Phase wird häufig sichtbar, wie sich Berechtigungen, Datenablagen und Arbeitsweisen über Jahre entwickelt haben. Typische Beispiele sind ehemalige Projektmitarbeitende mit weiterhin vorhandenen Zugriffsrechten oder die Nutzung von KI-Werkzeugen, für die bisher keine klaren Regeln definiert wurden.

Gleichzeitig geht es bei Governance nicht um mehr Bürokratie oder die Kontrolle von Mitarbeitenden. Klare Spielregeln und Sicherheitsmechanismen unterstützen Mitarbeitende dabei, im Arbeitsalltag sichere Entscheidungen zu treffen, beispielsweise beim Teilen von Informationen, beim mobilen Arbeiten oder beim Einsatz von KI. Folgende Maßnahmen helfen innerhalb kurzer Zeit:

- Sensibilisierung der Mitarbeitenden durch **Security-Awareness-Trainings**
- Etablierung von **sicheren Freigabe-, Zugriffs- und Freigabeprozessen**
- **Bereitstellung klarer Leitlinien für den Einsatz von Künstlicher Intelligenz und Cloud-Diensten**

Das Ergebnis nach 60 Tagen:

Kritische Zugriffe, Verantwortlichkeiten und Richtlinien sind klar definiert, Mitarbeitende erhalten Orientierung für den sicheren Umgang mit Daten, Cloud-Diensten und Künstlicher Intelligenz. Außerdem werden Risiken nicht nur erkannt, sondern aktiv und nachvollziehbar gesteuert. Allein durch die Bereinigung von Berechtigungen sowie die Einführung klarer Leitplanken für Cloud- und KI-Nutzung lässt sich das Risiko innerhalb weniger Wochen deutlich reduzieren.





Tag
61-90

PHASE 3: HANDLUNGSFÄHIGKEIT TESTEN

Spätestens jetzt sollte der Blick auf die entscheidende Frage gerichtet werden: „Was passiert eigentlich, wenn morgen etwas schiefgeht?

Wie viele Unternehmen verfügen sicher auch Sie über Datensicherungen und Notfallpläne. Wann haben Sie das letzte Mal getestet, ob diese im Ernstfall tatsächlich funktionieren? Deshalb steht in den letzten vier Wochen nicht die Planung, sondern das Testen im Mittelpunkt.

Typische Maßnahmen dieser wichtigen letzten Phase sind:

- Wiederherstellung wichtiger Daten testen
- Notfallrollen und Verantwortlichkeiten überprüfen
- Kommunikationswege für Krisensituationen abstimmen
- Cloud- und Dienstleisterabhängigkeiten bewerten
- Szenarien für Systemausfälle oder Cyberangriffe durchspielen
- Prioritäten für den Wiederanlauf des Geschäftsbetriebs festlegen

Ein wichtiger Part dabei ist die Simulation des Ausfalls eines Ihrer wichtigen Systeme wie z.B. das ERP-System. Wie wichtig ist bei Ihnen die Integration von Auftragsabwicklung, Lieferungen und Fakturierung? Durch diese Art von Übung entsteht innerhalb weniger Stunden ein wesentlich klareres Verständnis darüber, welche Systeme und Informationen im Ernstfall zuerst verfügbar sein müssen.

Das Ergebnis nach 90 Tagen:

Sie kennen Ihre größten Risiken, haben klare Verantwortlichkeiten geschaffen und wichtige Notfallszenarien bereits praktisch überprüft. Aus vielen Einzelmaßnahmen ist ein gemeinsames Verständnis darüber entstanden, welche Informationen, Systeme und Prozesse für Ihr Unternehmen wirklich kritisch sind.

Vor allem aber gewinnen Sie etwas, das in einer zunehmend digitalen Welt immer wichtiger wird: die Sicherheit, die richtigen Entscheidungen treffen zu können und auch in schwierigen Situationen handlungsfähig zu bleiben.

Die wichtigste Erkenntnis wird sein: Der 90-Tage-Plan ist kein Projektende. Er markiert vielmehr den Beginn eines kontinuierlichen Verbesserungsprozesses. Denn Unternehmen, die ihre Risiken kennen, klare Spielregeln etablieren und ihre Handlungsfähigkeit regelmäßig überprüfen, schaffen die Grundlage für einen sicheren, resilienten und zukunftsfähigen Geschäftsbetrieb.





FAZIT:

CHANCEN NUTZEN & RISIKEN BEHERRSCHEN



Je stärker Unternehmen digital arbeiten, desto wichtiger wird die Frage, wie Informationen geschützt, Zugriffe gesteuert und geschäftskritische Prozesse abgesichert werden. Dabei geht es nicht darum, jede denkbare Gefahr auszuschließen oder jede Technologie selbst zu betreiben.

Entscheidend ist vielmehr, den Überblick zu behalten, die richtigen Entscheidungen zu treffen und auch dann handlungsfähig zu bleiben, wenn nicht alles nach Plan läuft.

Unternehmen, die Sicherheit, Governance und Handlungsfähigkeit gemeinsam betrachten, schaffen die Grundlage für nachhaltiges Wachstum, Vertrauen und Wettbewerbsfähigkeit.

Wir helfen Ihnen dabei, zu jeder Zeit im Driver Seat zu bleiben. Sprechen Sie uns einfach an, wir freuen uns auf Sie!

verkauf@it-improvement.com

Telefon: 0202/440 968 30

Oder besuchen Sie unsere kostenfreien Webinare!

Auf unserer Eventseite finden Sie alle Termine inklusive Anmeldung:

Events & Webinare

Ihr pragmatischer Start:

Der wichtigste Schritt ist oftmals der erste.

Sie müssen nicht sofort jedes System modernisieren, jede Richtlinie neu schreiben oder sämtliche Prozesse neu gestalten. Beginnen Sie dort, wo der größte Nutzen entsteht: bei den Informationen, Prozessen und Risiken, die für Ihr Unternehmen wirklich kritisch sind.

Gemeinsam analysieren wir Ihren Status quo, identifizieren die größten Hebel und entwickeln einen praxisnahen Improvement-Plan, der zu Ihrem Unternehmen, Ihren Ressourcen und Ihren Geschäftszielen passt.

Lassen Sie uns gemeinsam dafür sorgen, dass Ihr Unternehmen auch morgen sicher, resilient und handlungsfähig bleibt.

 **Microsoft**
Solutions Partner
Modern Work

 **Microsoft**
Solutions Partner
Data & AI
Azure

 **Microsoft**
Solutions Partner
Digital & App Innovation
Azure

 **Microsoft**
Solutions Partner
Security

 **Microsoft**
Solutions Partner
Infrastructure
Azure

 **Microsoft**

powered by

