## LEISTUNGEN

# *In drei Schritten zum Erfolg*

**1. BESTANDSAUFNAHME VOR ORT (DAUER 1 – 2 TAGE)**
- Checklisten-gestützte Ist-Aufnahme
- nichtinvasive Sichtprüfung von Konfigurationen
- Interviews mit Geschäftsleitung, iT-Verantwortlichen und Anwender*innen

**2. ANALYSE UND AUSWERTUNG**
- Bewertung der fünf Risikokategorien: Ausfallwahrscheinlichkeit, Ausfalldauer, Datenverlust, interne und externe Verwundbarkeit
- Erstellung von Handlungsempfehlungen
- Visualisierung der Netzwerkinfrastruktur
- Zusammenfassung der Ergebnisse

**3. RIT® iT RISK ASSESSMENT WORKSHOP**
- Executive Summary für die Geschäftsführung (Dauer: 1/2 Std.)
- Detailbericht für die iT-Verantwortlichen (Dauer 3 – 4 Std.)
- Abstimmung nächster Maßnahmen und Prioritäten

## KONTAKT

# *Ihr Ansprechpartner Jetzt anfragen*


**MARKUS RÜPING**
Leitung
Infrastrukturmanagement
**rueping@RiT.de**


Mehr Informationen zum RIT® iT Risk Assessment

**R.iT – DISCOVER THE SPIRIT OF EXCELLENCE**

Die Digitale Transformation ist allgegenwärtig. Es gibt wohl kaum etwas, das unsere Wirtschaft und die Gesellschaft derart grundlegend verändern wird, wie dieser Prozess. Wir von R.iT beraten seit mehr als 20 Jahren Mittelstandsunternehmen auf diesem Weg und wir machen auch Sie zum **“Digital Champion: Made in Germany“**.


**R.iT GmbH**
Lise-Meitner-Allee 37, 44801 Bochum
+49 (234) 43 88 00-0
info@RiT.de | www.RiT.de


DISCOVER THE SPIR.iT OF EXCELLENCE.
*SURPASS YOUR SUCCESS.*

# *RIT® iT Risk Assessment Entscheidungsfähig in einem Tag*

*Übersicht für Geschäftsführung und iT-Entscheider*innen über den Status Ihrer iT-Sicherheit*


DISCOVER THE SPIR.iT OF EXCELLENCE.
*SURPASS YOUR SUCCESS.*

# Profitieren Sie von “Cybersecurity Made in Europe!”

Immer mehr Entscheider*innen wird bewusst, dass iT-Sicherheit nicht nur für das Tagesgeschäft wichtig ist, sondern auch eine notwendige Voraussetzung für die erfolgreiche Digitalisierung und insbesondere für den Erhalt der Wettbewerbsfähigkeit des eigenen Unternehmens darstellt. Systemausfälle und Datenverluste beeinträchtigen die Effizienz der Mitarbeiter*innen und gefährden langfristige Geschäftsmodelle. Angesichts der zunehmenden Berichte über Cyberangriffe und iT-Risiken stellt sich die Frage, wie gut Ihr Unternehmen geschützt ist und wie es auf potenzielle Vorfälle reagieren kann.

Unser **RIT® iT-Risk-Assessment** bietet Ihnen einen schnellen Überblick über den aktuellen Sicherheitsstatus Ihrer Unternehmens-iT sowie konkrete Handlungsempfehlungen zur nachhaltigen Verbesserung.


**aller deutschen Unternehmen sind vom Diebstahl von Daten sowie von digitaler Industriespionage oder Sabotage betroffen.**

*Quelle: Bitkom Research 2024*
*(Zeitraum: letzte 12 Monate)*

### Für Geschäftsführer*innen

Als primär kaufmännisch verantwortliche*r Vorstand oder Geschäftsführer*in profitieren Sie von einem RIT® iT-Risk-Assessment, das Ihnen eine präzise Analyse der Risiken in Ihrer iT-Infrastruktur bietet. Es zeigt Ihnen gezielt auf, in welchen Bereichen Handlungsbedarf besteht, **wie Sie Risiken minimieren können und welche Investitionen dafür erforderlich sind**.

### Für (iT-)Sicherheitsverantwortliche

Ein RIT® iT-Risk-Assessment liefert Ihnen eine fundierte Status-Quo-Analyse als **Grundlage zur Erstellung oder Aktualisierung Ihres iT-Sicherheitskonzepts** und zur gezielten Priorisierung wirksamer Maßnahmen.

### Für iT-Leiter*innen

Mit Unterstützung eines erfahrenen externen Experten oder einer Expertin überprüfen Sie die iT-Sicherheit Ihrer Infrastruktur, identifizieren systematisch Sicherheitslücken und **entwickeln gezielte Maßnahmen** – basierend auf einem RIT® iT-Risk-Assessment.

## Ihre persönliche Auswertung

In unserem **RIT® iT-Risk-Assessment Workshop** erhalten Sie eine Bewertung Ihrer Sicherheitslandschaft. Hierdurch bekommen Sie ein transparentes Lagebild, und die iT-Risiken werden konkret benannt und nach Wichtigkeit und Dringlichkeit kategorisiert. Zusätzlich stellen wir Ihnen einen Detailbericht für Ihre iT-Sicherheitsverantwortlichen und stimmen mit Ihnen Maßnahmen und Prioritäten ab.

### Beispielbewertung


### Beispiele für Handlungsempfehlung

| Priorität | empfohlene Maßnahme | (Risiko-)Bereich |
|---|---|---|
| 1 | Datensicherungskonzept erstellen und umsetzen | Datenverlust, Ausfalldauer |
| 2 | internes anonymes Versenden von E-Mails unterbinden | externe Verwundbarkeit |
| 3 | Benutzern Administrator-Rechte entziehen | interne Verwundbarkeit |
| ... | | |

**AUSGEZEICHNETE REFERENZEN**

CYBERSECURITY MADE IN EUROPE™