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

Die letzte leichte Beute: Warum Cybersicherheit für den Mittelstand jetzt zur Überlebensfrage wird

ILEP-Community-Webinar

Tobias Rademann

28. Oktober 2026


1. Was da draußen passiert

Demo

an dieser Stelle wurde während des Vortrags ein simulierter Cyberangriff mittels einer ClickFix-Attacke gezeigt.

© R.iT GmbH, 2026

Das war's!

Ihre Daten sind jetzt *weg.*

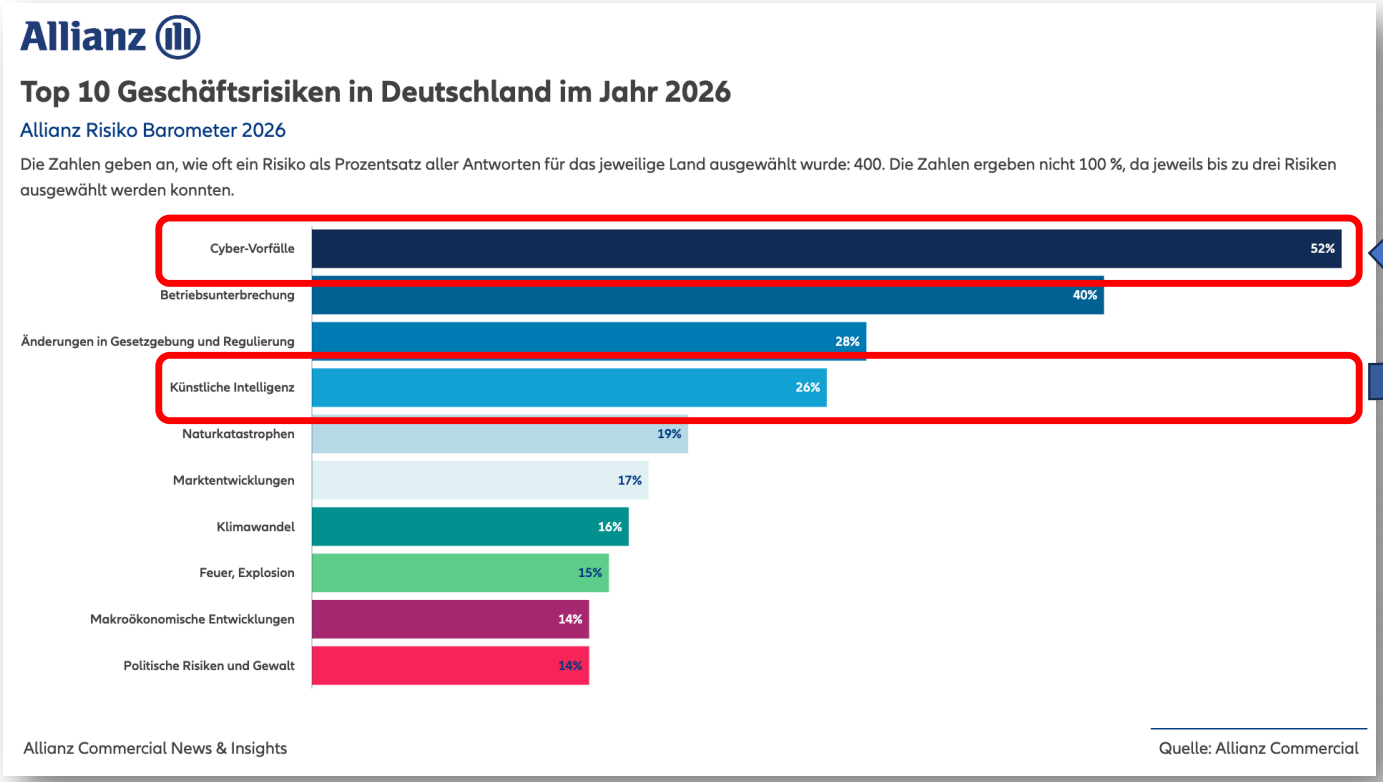
Ihre Systeme stehen *still.*

Ihre Kunden
bekommen *Angst*...

...und wenden sich ab.

Ihr Lebenswerk
steht jetzt
zur Verhandlung.

Cyber-Vorfälle = Unternehmensrisiko Nr. 1



https://app.23degrees.io/view/MsBjQWIRj5ZtmCUd-bar-horizontal-top-10-geschaeftsrisiken-in/

KI macht Angriffe

- günstiger
- häufiger
- schneller
- und erfolgreicher

Agenda

1. *Demo: Cyberangriff*
2. Wie ein Angriff abläuft
3. Die Wahl der Opfer – gezielt oder Zufall?
4. Trügerische Sicherheit
5. Warum NIS-2 die Bedrohungslage verschiebt
6. Was Sie jetzt tun können
7. Fazit



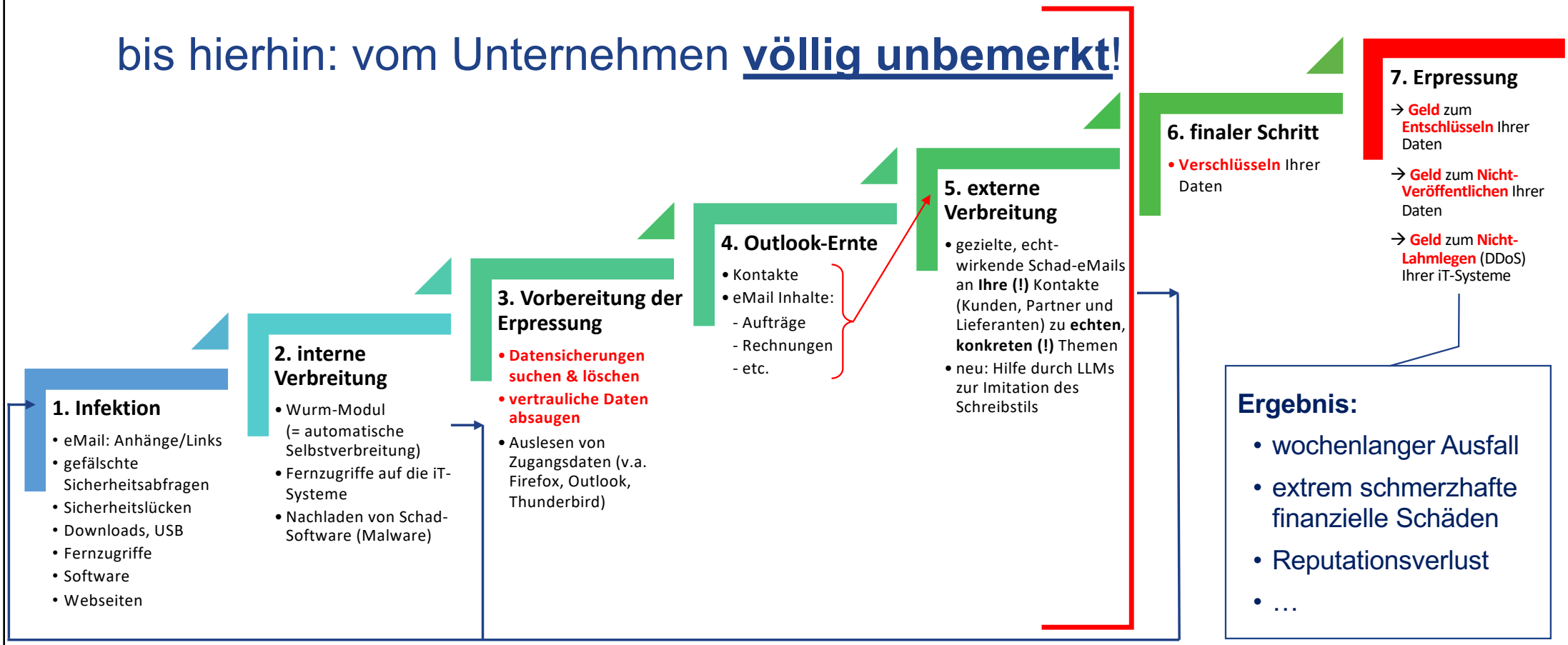
© R.iT GmbH, 2026



2. Wie ein Angriff abläuft

Erpressungstrojaner 4.0 ('Triple Extortion')

bis hierhin: vom Unternehmen **völlig unbemerkt**!



© R.iT GmbH, 2026



3. Die Wahl der Opfer – gezielt oder Zufall?

Die Diebe fragen nicht, wer wo wohnt. Sie testen, ob die Tür aufgeht.

Seit Jahren: Täter rütteln an jeder Tür – automatisch

Das belegen die Zahlen:

- ~6.000 Honeypot-Fallen (Telekom 2025):
  65 Mio. Angriffe / Tag auf Fallen, die **nichts** enthalten und die **niemand** kennt
- 2017: 4 Mio. → 2019: **31 Mio.** → 2025: **65 Mio.**
  Das Fließband beschleunigt sich!
- Neuer Server in Frankfurt: Erster Angriffsversuch nach 1h (Sophos, 2019)
- 119 neue Schwachstellen pro Tag (BSI-Lagebericht 2025)

➔ Das machen keine Menschen, das machen Programme –
Tag und Nacht, jede Adresse im Internet

© R.iT GmbH, 2026

Seit Jahren: Täter rütteln an jeder Tür – automatisch

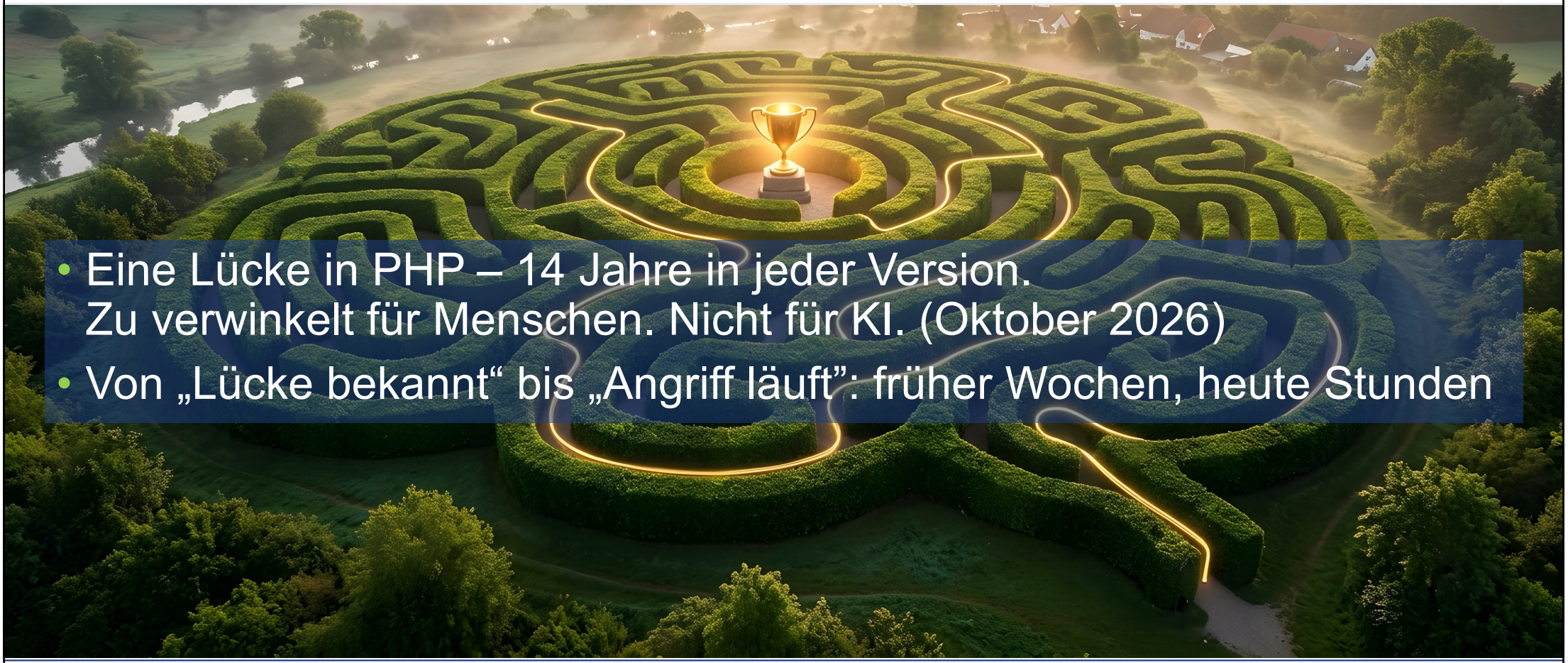


© R.iT GmbH, 2026

Das Fließband gibt es seit Jahren.
Neu ist: Es bekommt ein Gehirn.



Seit Kurzem: Wege, die 14 Jahre niemand fand

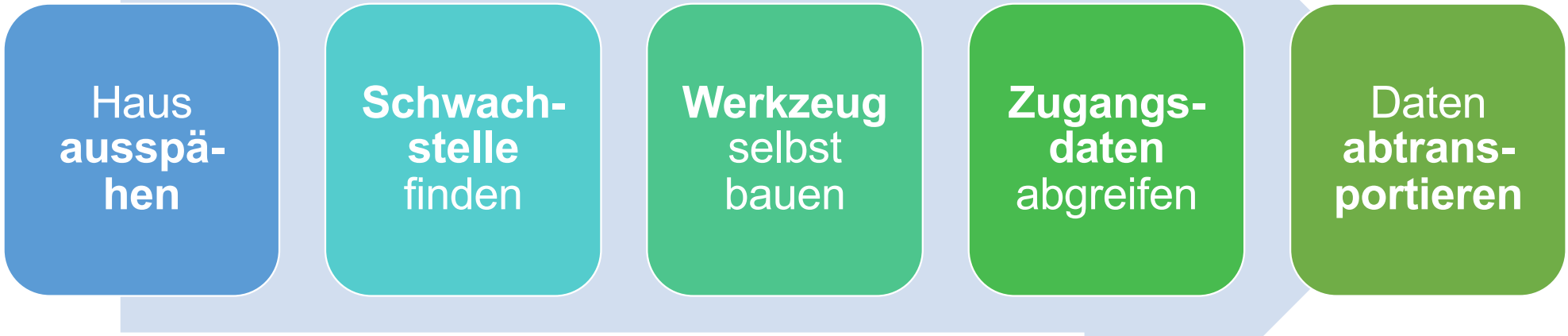


- Eine Lücke in PHP – 14 Jahre in jeder Version.
  Zu verwinkelt für Menschen. Nicht für KI. (Oktober 2026)
- Von „Lücke bekannt“ bis „Angriff läuft”: früher Wochen, heute Stunden

© R.iT GmbH, 2026

Jetzt: Dieselben Schritte wie bisher – nur ohne Mensch

Angriff in fünf Schritten:



Alles von der KI. Der Mensch gibt max. noch frei. *(Quelle: Anthropic, 11/2025)*

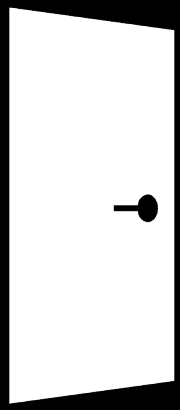
© R.iT GmbH, 2026

Der Täter muss Sie nicht (mehr) kennen.
Seine Maschine findet Sie – wenn Ihre Tür aufgeht.

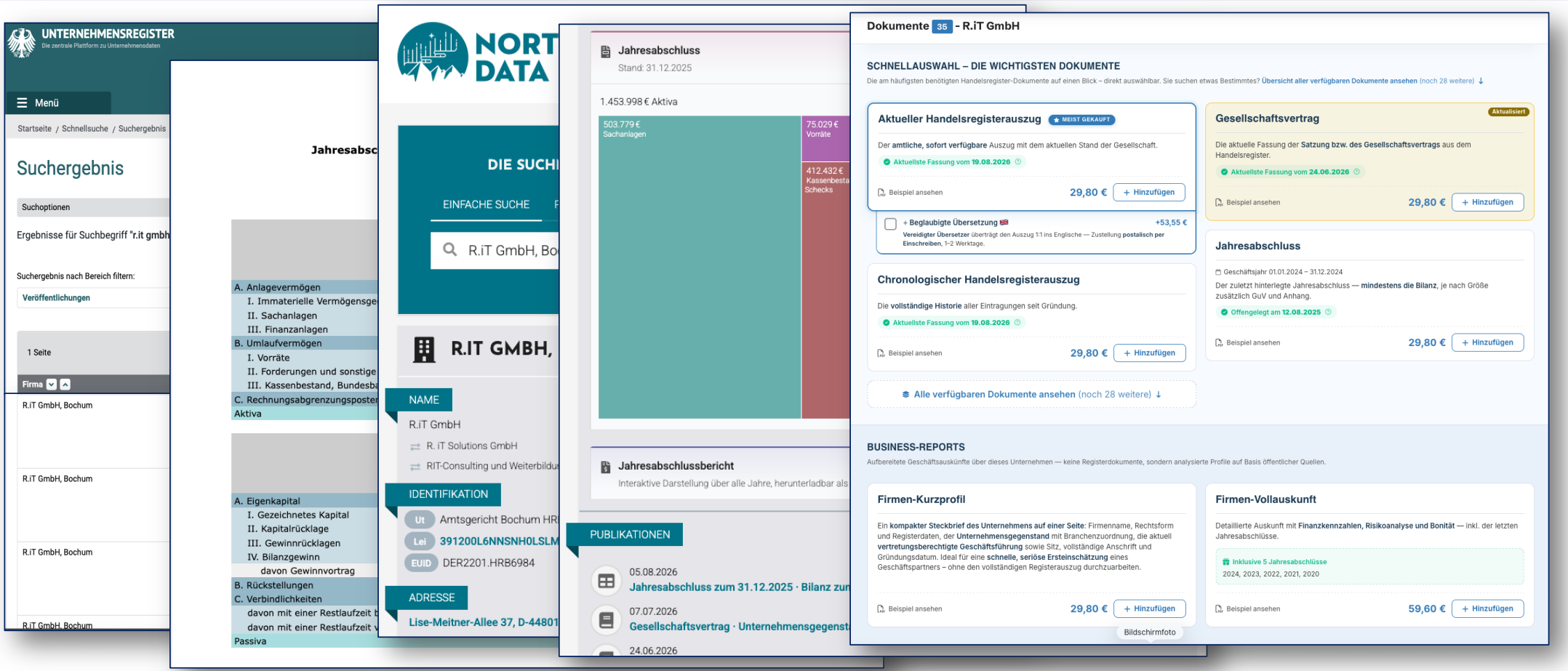
Nicht Ihre Bedeutung entscheidet.
Sondern der Zustand Ihrer Tür.

Und wenn die Tür aufgeht?

Dann weiß er, **was Sie sich leisten können –**
***bevor* er die Rechnung schreibt.**

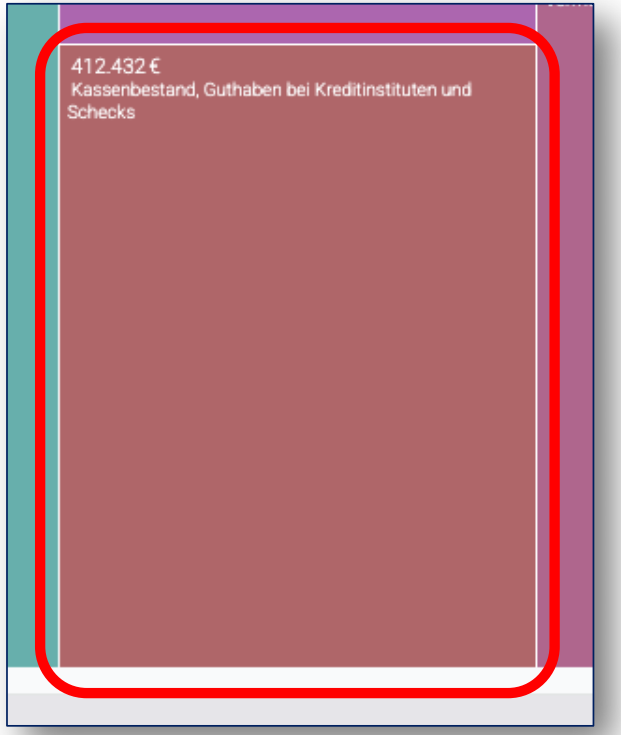


Das findet ein Angreifer in fünf Minuten



© R.iT GmbH, 2026

Sie erinnern sich an meine Aussage von gerade?



© R.iT GmbH, 2026

Und wo eine Tür aufging, kommt die Bande wieder…

Sanitätshausbranche

- rahm: 09/2025 (50 NL, > 2 Mio. Kunden)
- RehaVital: 07/2026 (950+ Standorte)
- zwei weitere Häuser: Forderungen über $ 5 / $ 27 Mio.

➔ Die Branche *re*-agiert aufgeschreckt:
Webinare, Warnungen, kurzfristig einberufene Krisenformate

➔ Die $ zeigen: Die Rechnung kommt nicht aus Deutschland –
und die Täter kannten vermutlich keine der o.g. Firmen!

Vier Vorfälle. Zehn Monate. Eine Branche.

© R.iT GmbH, 2026



4. Trügerische Sicherheit

Fall aus unserer Praxis

Angebotsbesprechung 'iT Risk Assessment'

- R.iT: "Dann werden wir uns auch Ihre **Datensicherung** anschauen."
- Kunde: "Nein, die läuft problemlos. Wir haben schon zig Dateien wiederhergestellt, hier ist **definitiv kein Bedarf**."

2 Tage später: Anruf vom Kunden

- Kunde: "Können Sie uns bei einem **iT-Sicherheitsvorfall** helfen? Wir wurden gehackt. An unsere Kunden und Lieferanten wurden zudem mehrere hundert Schad-eMails verschickt."
- R.iT: System **seit drei Wochen kompromittiert**.
  Datensicherung: Historie: **nur 1 Woche**
  Umfang: **lückenhaft**; Cloud fehlte **vollständig**

© R.iT GmbH, 2026

weiterer Fall aus unserer Praxis

- **Vorbesprechung mit dem iT-Dienstleister:**
  - Die Server **laufen** seit Jahren.
  - Das System ist **sicher**.
  - Die Datensicherung haben wir sogar **doppelt** ausgelegt.

- **Ergebnis unserer Prüfung:**
  - Das System war **seit > 8 Wochen kompromittiert (= gehackt)**.
  - Die zentrale Datensicherung lief **seit über sechs Wochen (!)** nicht.
  - Das Kennwort für den Zugriff auf die Datensicherung lag **im Klartext** vor.
  - Eine offsite-Datensicherung war **nicht vorhanden**.

© R.iT GmbH, 2026

Es ist keine Frage der Sorgfalt

Bei iT-Sicherheit macht **niemand** (!)
absichtlich und ***bewusst*** etwas falsch!

Gründe für Fehler:

- fehlendes Wissen
- fehlende Erfahrung
- Flüchtigkeitsfehler

© R.iT GmbH, 2026

iT ≠ iT-Sicherheit: Zwei Fachrichtungen

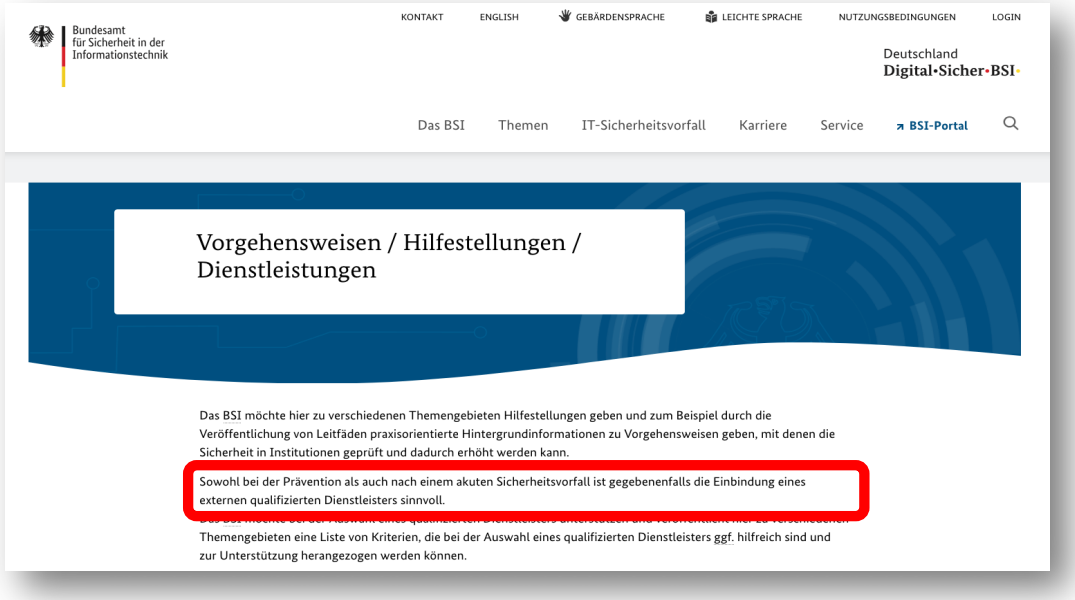
	iT	iT-Sicherheit
Die Frage	Läuft es?	**Hält es stand?**
Der Blick	wie der Nutzer	**wie der Angreifer**
Erfolg heißt	keiner ruft an	**keiner kommt rein**
Im Konflikt gewinnt	die Bequemlichkeit	**die Hürde**
Das Vorbild	der Architekt	**der Statiker**

Und egal, wie gut beide sind: Niemand prüft seine eigene Arbeit.
Deshalb gibt es Buchhalter und Wirtschaftsprüfer.

© R.iT GmbH, 2026

Der Blick von außen

Selbst das BSI empfiehlt, für Prävention wie Ernstfall einen **qualifizierten externen Dienstleister** einzubinden:



Quelle: BSI, „Vorgehensweisen / Hilfestellungen / Dienstleistungen", https://bsi.bund.de/dok/6781784

© R.iT GmbH, 2026

Das Gefährlichste ist nicht die Lücke.

Es ist der Glaube, keine zu haben.



5. Warum NIS-2 die Lage verschiebt

NIS-2: generelle Betroffenheit

Betroffen ist, wer **beides** erfüllt:

in reguliertem* Sektor tätig

**einer der 14 Sektoren nach Anlage 1 oder 2*

UND

ab 50 Beschäftigten

oder

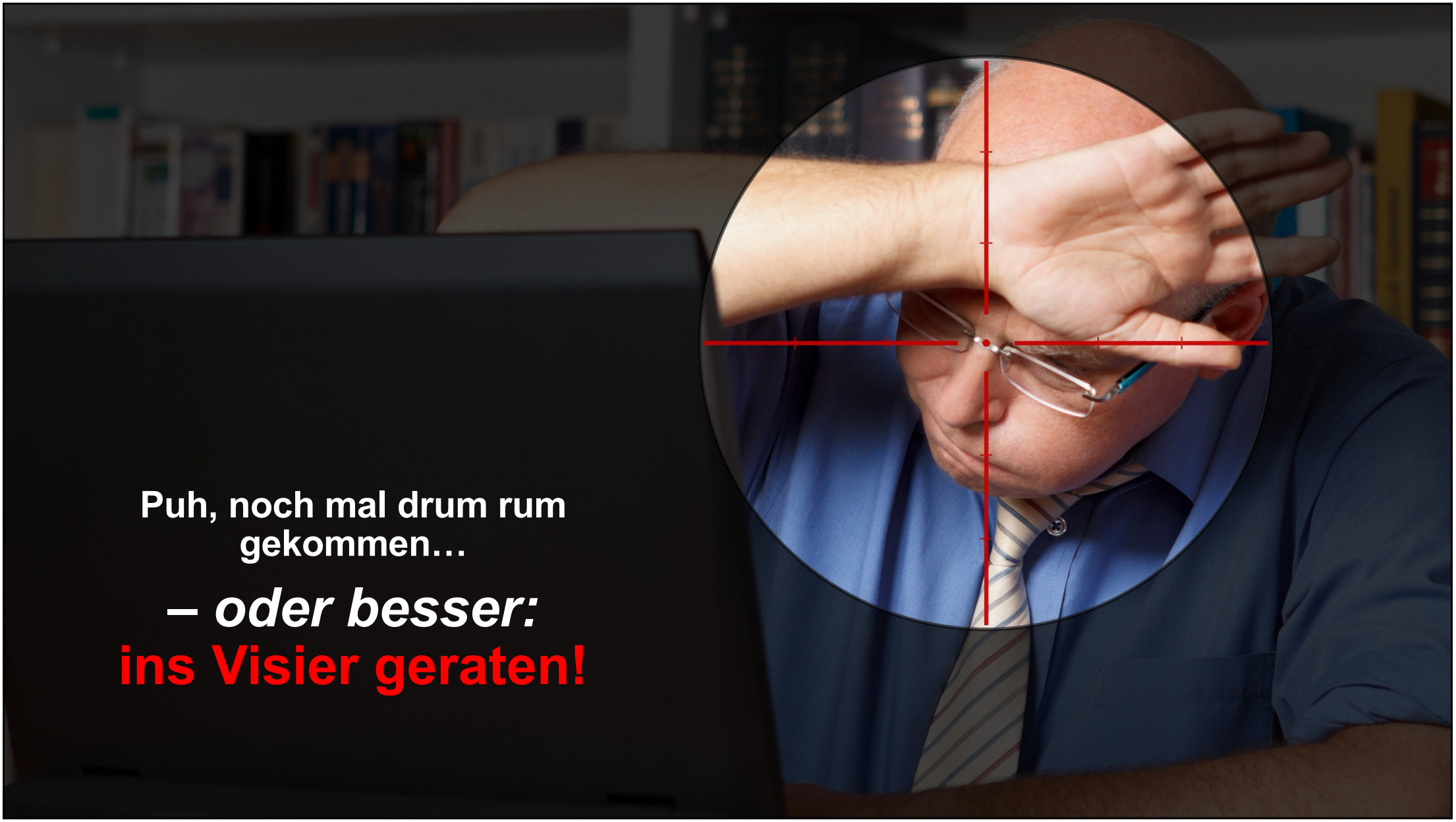
> €10 Mio. Umsatz und Bilanzsumme

(in zwei aufeinanderfolgenden Jahren)

vereinfachte Darstellung

© R.iT GmbH, 2026


Puh, noch mal drum
rum gekommen…


Puh, noch mal drum rum gekommen…
– *oder besser:*
ins Visier geraten!

Ins Visier geraten

Schutzquote steigt

- NIS-1/KRITIS: 4.500 KRITIS-Anlagen mussten abgesichert werden
- NIS-2: 30.000 Mittelständler müssen handeln

Der ungeschützte Rest:

erreichbar, weitgehend wehrlos – und oft zahlungsfähig

→ **unvergleichlich attraktiv für Angreifer**

KI senkt die Angriffskosten *und* steigert Erfolgswahrscheinlichkeit

automatisierte und zielgerichtete Angriffe werden möglich und lohnend

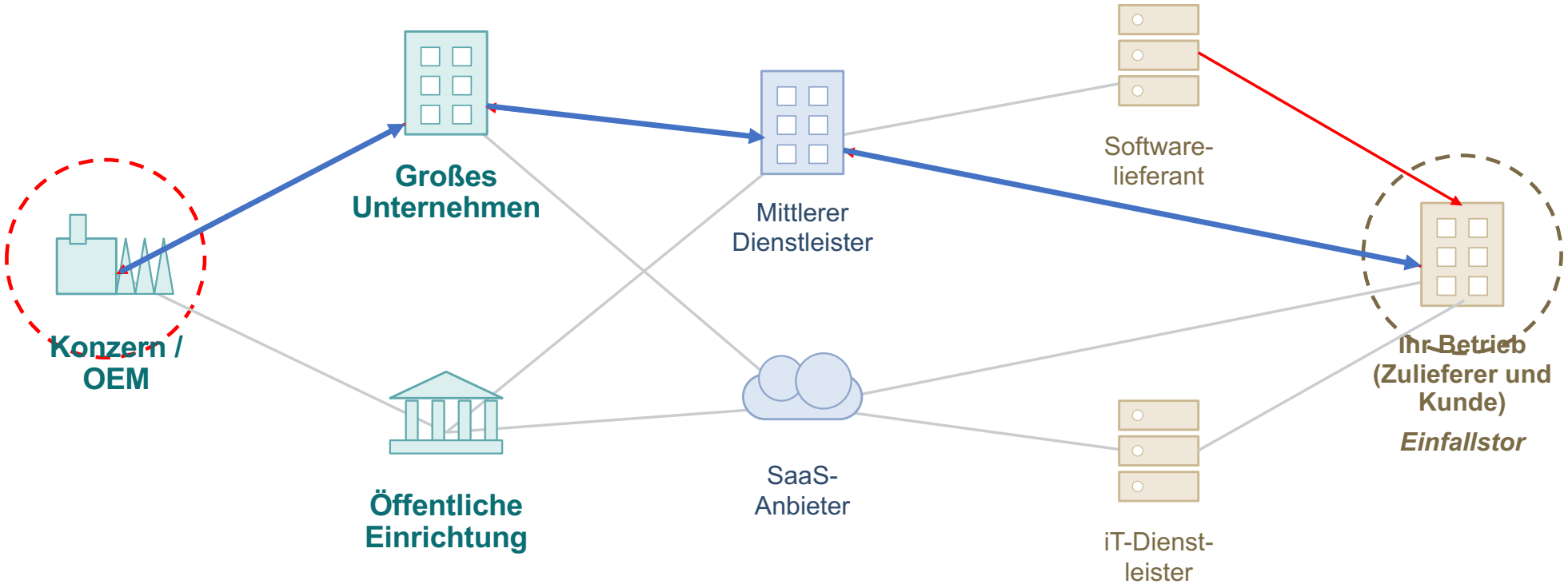
© R.iT GmbH, 2026

…und der Rest steht auf der Tageskarte



© R.iT GmbH, 2026

Der Druck „von oben“: Sicherheit der Lieferkette



***Angriff* fließt nach oben – die *Anforderung* nach unten**: Ihre Kunden fordern Sicherheit von Ihnen ein.

© R.iT GmbH, 2026



6. Was Sie jetzt tun können

Was Sie jetzt tun können

Schritt 1: Ihre Rolle

Schritt 2: Ihr Standort und Ihre Prioritäten

Schritt 3: Umsetzung beginnen

Schritt 4: Ihren Ernstfall proben

© R.iT GmbH, 2026

Schritt 1: Ihre Rolle – Steuerung übernehmen

iT-Sicherheit ist ***kein*** **iT-Thema**.

Es ist **Risikomanagement**.

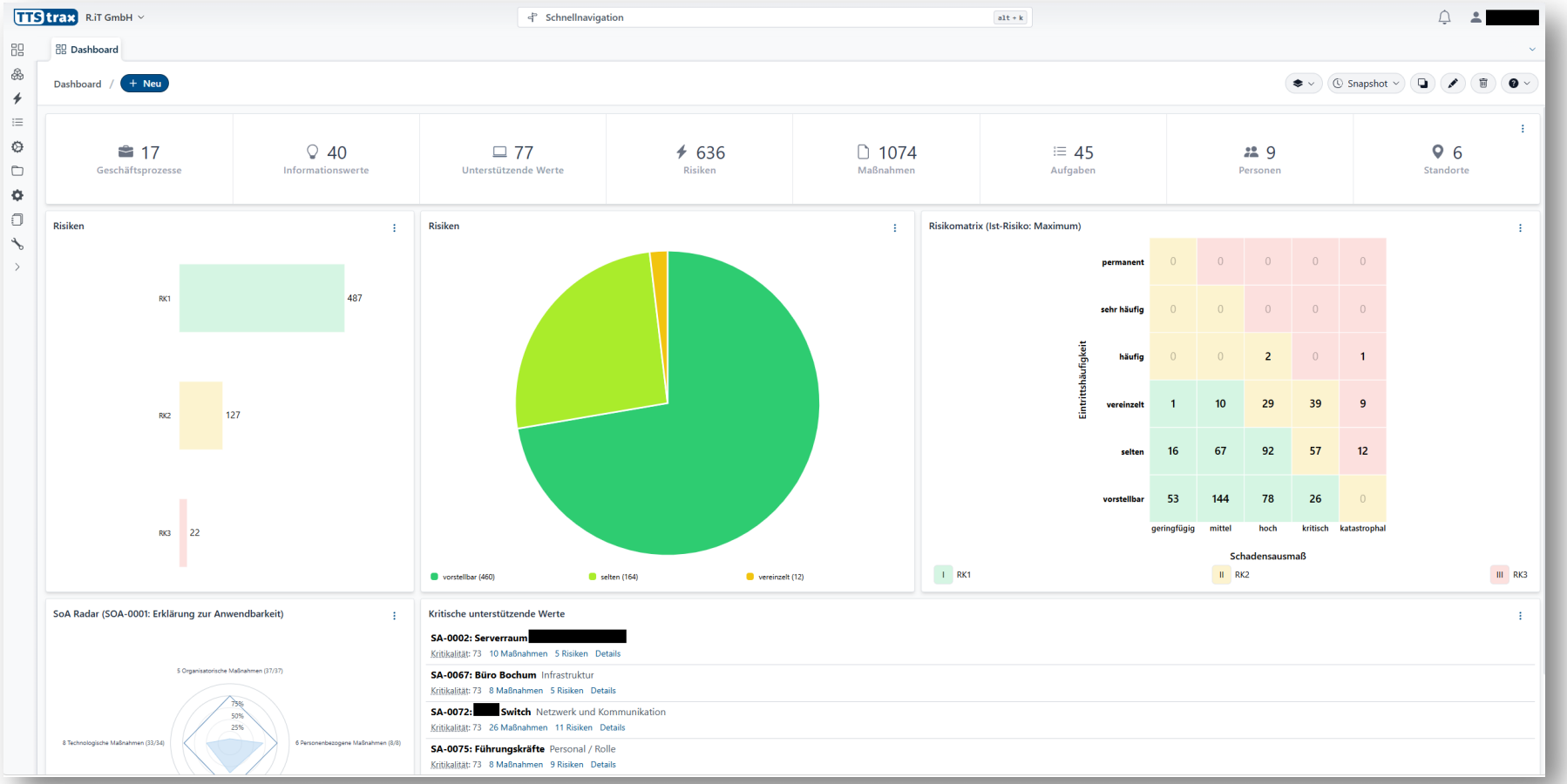
→ Und damit Ihre Kerndisziplin.

Ihre Geschäftsrisiken:

Liquidität • Personal • iT-Sicherheit

© R.iT GmbH, 2026

Schritt 1: So sieht gelebtes Risikomanagement aus



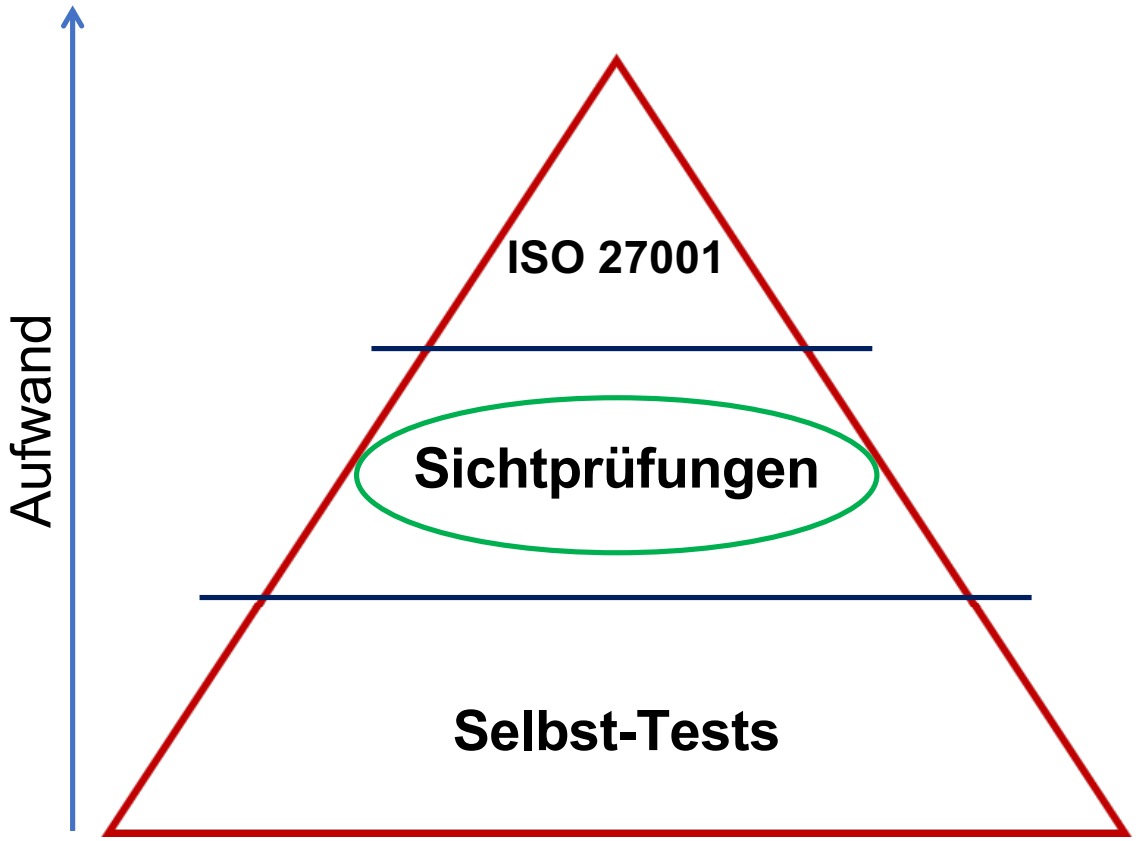
Schritt 2: Standort bestimmen

Sie können nicht schützen,
was Sie nicht kennen.

→ Risiken **sichtbar machen** *und*
→ Dringlichkeit **bewerten** (priorisieren)

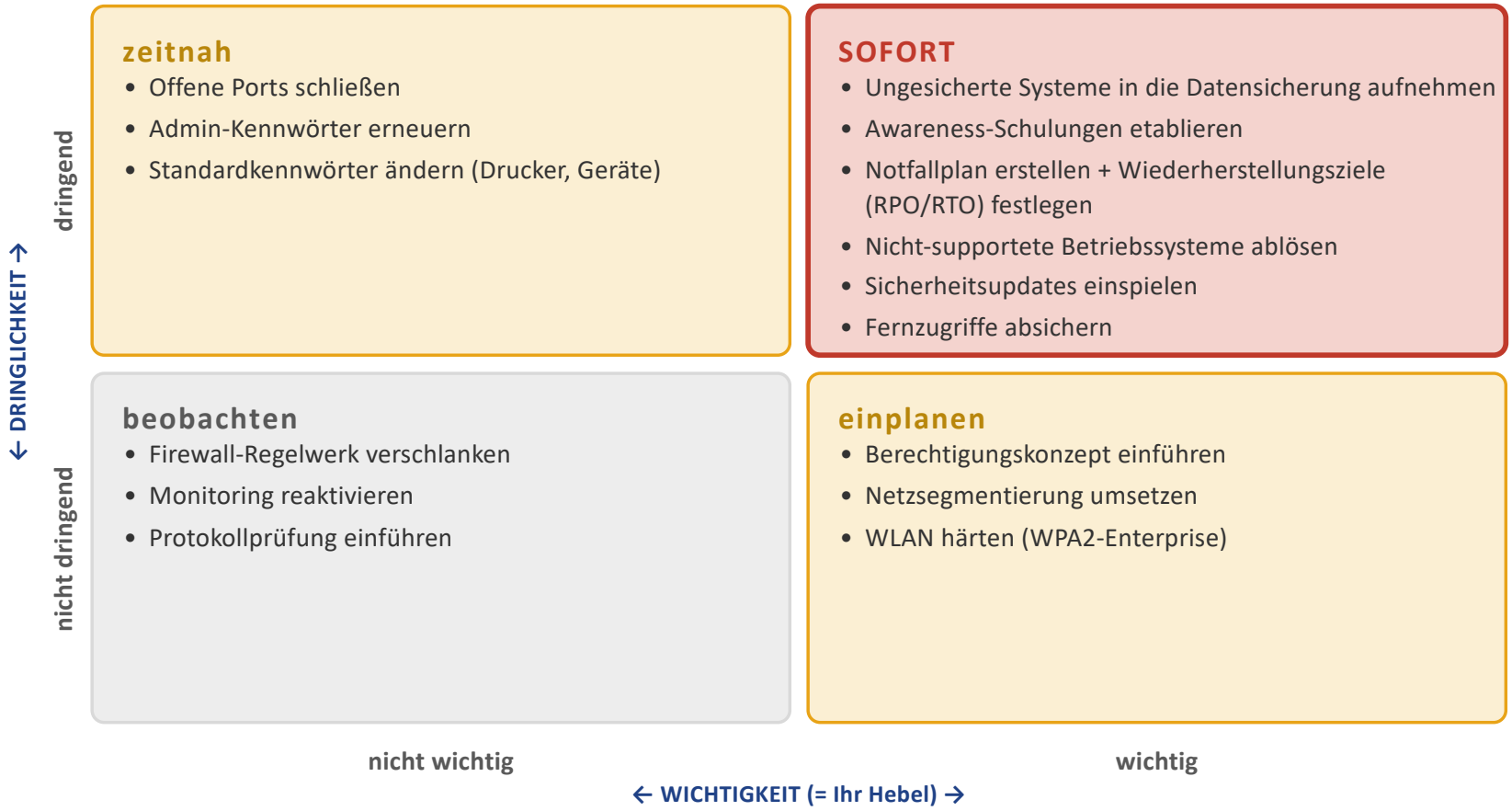
© R.iT GmbH, 2026

Schritt 2: Drei Wege zum Überblick



© R.iT GmbH, 2026

Schritt 2: Das Ergebnis: Ihre iT-Risiken – priorisiert



© R.iT GmbH, 2026

Schritt 3: Must-haves – ohne sind Sie leichte Beute

Die Basis – bei fast allen unserer Prüfungen steht sie ganz oben rechts in der Matrix. Reihenfolge = Reihenfolge der Umsetzung.

	Maßnahme	Wirkung	Aufwand
1	**Datensicherung** Drei Kopien, eine offline. Rückspielen regelmäßig testen.	●●●	●○○
2	**Sicherheitsupdates** Kritische in 48 h, Rest in 14 Tagen. Altes ersetzen.	●●●	●●○
3	**Multi-Faktor-Authentifizierung** Zweiter Faktor auf jedem Zugang von außen.	●●●	●●○
4	**Keine Admin-Rechte im Tagesgeschäft** Mails und Surfen nur als normaler Nutzer. Auch die Chefs.	●●●	●○○
5	**Zentraler Endgeräteschutz (EDR)** Erkennt Verhalten, nicht nur Viren. Einbrecher nach Minuten statt Wochen.	●●○	●●●
6	**Mitarbeiter sensibilisieren** Zweimal im Jahr kurz schulen, dazwischen Phishing-Tests.	●●○	●○○
7	**Notfallplan** Eine Seite auf Papier: wer entscheidet, wer anruft, was zuerst. Jährlich durchspielen.	●●●	●○○

Wirkung: Schutz vor den häufigsten Angriffswegen · Aufwand: Kosten und interne Zeit für ein Unternehmen mit 20–200 Mitarbeitern

© R.iT GmbH, 2026

Schritt 3: Die nächste Stufe

Mehr Schutz, mehr Aufwand – sinnvoll erst, wenn die sieben Must-haves wirklich laufen. Nicht vorher.

Maßnahme	Wirkung	Aufwand
1 Berechtigungskonzept & Netzsegmentierung Jeder sieht nur, was er braucht. Produktion, Büro und Gäste in getrennten Netzen.	●●●	●●○
2 E-Mail-Schutz Weniger Phishing im Postfach – und Ihre Adresse lässt sich nicht mehr fälschen.	●●○	●○○
3 Passwort-Manager & Passkeys Ein starkes Passwort pro Dienst, ohne es sich merken zu müssen.	●●○	●○○
4 Verschlüsselung & Verwaltung mobiler Geräte (MDM) Jedes Notebook und Handy verschlüsselt und aus der Ferne löschbar, kein Datenvorfall.	●●○	●●○
5 Zugriffsbedingungen (Conditional Access) Anmeldung nur von bekannten Geräten und plausiblen Orten. Alles andere wird blockiert.	●●○	●●○
6 Überwachung rund um die Uhr (MDR / SOC) Externe Spezialisten überwachen Ihr Netz 24/7 und greifen bei Alarm ein. Auch nachts, auch sonntags.	●●●	●●●
7 Dienstleister & Lieferanten prüfen Wer Zugang zu Ihren Systemen hat, weist Sicherheit nach.	●●○	●○○

Wirkung: zusätzlicher Schutz über die Basis hinaus · Aufwand: Kosten und interne Zeit für ein Unternehmen mit 20–200 Mitarbeitern

© R.iT GmbH, 2026


Schritt 4: Ihren Ernstfall üben
Wie überweisen wir Bitcoins?


Schritt 4: Ihren Ernstfall üben / II
Was machen wir, wenn
– keine Telefone
– keine eMails
– keine Website
– etc.
mehr funktionieren und uns unsere Kunden nicht erreichen können?

Schritt 4: Drei Phasen – auf alle drei vorbereitet

Ein Angriff ist kein Moment, sondern drei Phasen. Jede stellt andere Fragen – und jede lässt sich vorher durchdenken.

VOR dem Angriff

***Jetzt. Solange noch Zeit ist*:**

„Wo stehen wir – und was zuerst?“

Vorher durchdenken:

- Must-haves umgesetzt, Backup getestet
- Notfallplan geschrieben – auf Papier
- Erreichbarkeiten geklärt:
  Dienstleister, Versicherung, Anwalt, Polizei
- Ernstfall geprobt (Tabletop)

WÄHREND des Angriffs

***Stunden. Unter Druck, ohne IT*:**

„Was tun wir jetzt – und wer?“

Vorher durchdenken:

- Wer entscheidet – und wer zieht den Stecker?
- Wen rufen wir in welcher Reihenfolge an?
- Zahlen oder nicht?
  Vorher festlegen, nicht nachts um drei
- Meldepflichten: 24 h (NIS-2), 72 h (DSGVO)

NACH dem Angriff

***Tage bis Monate. Das Geschäft muss weiterlaufen*:**

„Wie werden wir wieder arbeitsfähig – und wie bleiben wir es? “

Vorher durchdenken:

- Wie arbeiten wir ohne Telefon, Mail, Website?
  Papier, Handy, Notbetrieb
- Wer informiert Kunden, Lieferanten, Mitarbeiter – und wie, ohne Mail?
- Wiederanlauf: welches System zuerst?
- Was lernen wir – und was ändern wir?

**Vorbereitet oder nicht – das entscheidet:
fünf Tage Stillstand oder Insolvenz.**

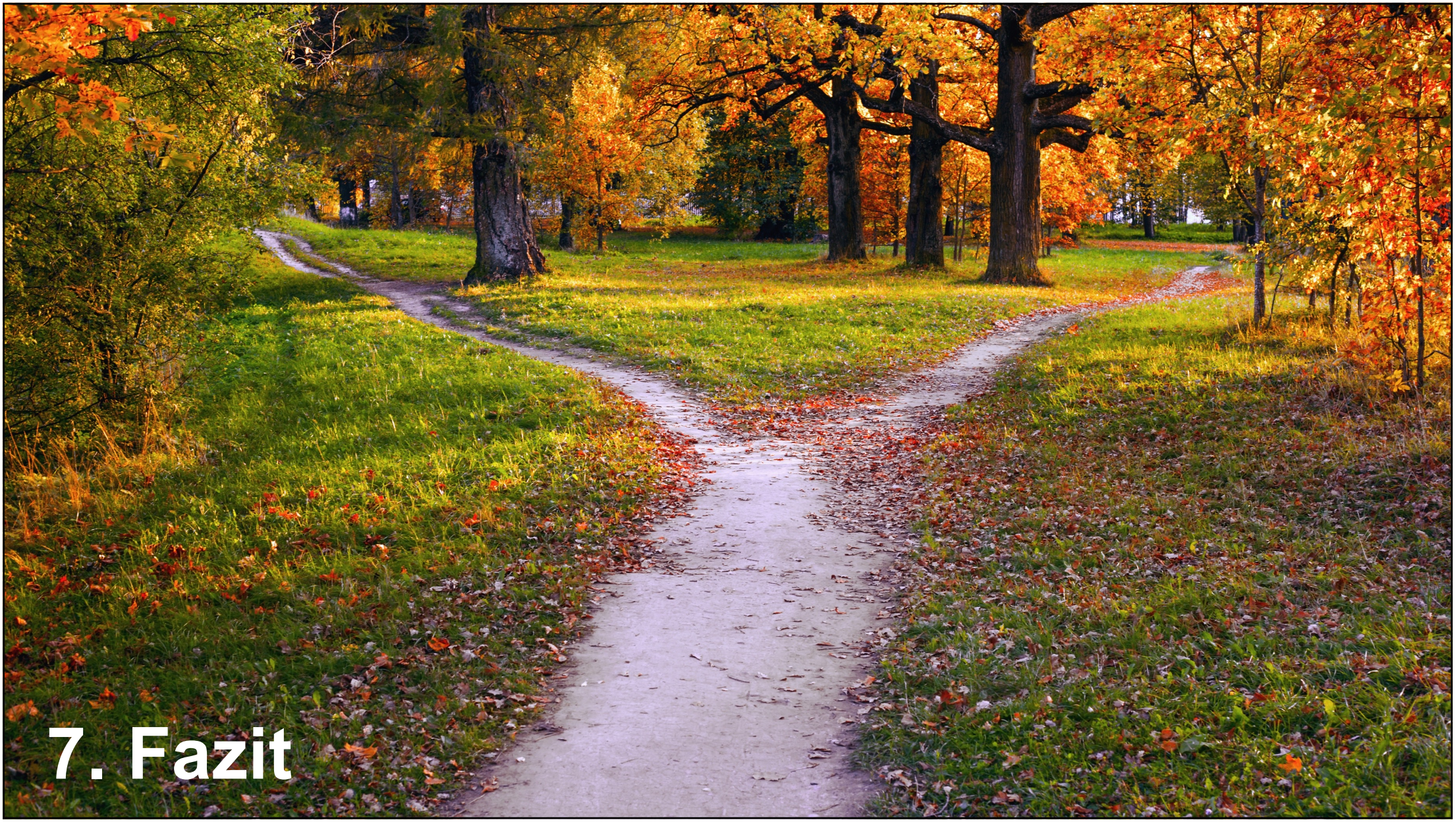
© R.iT GmbH, 2026

Alles, was wir besprochen haben
– priorisiert, systematisch, im Kreislauf gesteuert – hat einen Namen:



Ihr Fahrplan zu systematischer iT-Sicherheit – geschenkt!

© R.iT GmbH, 2026


7. Fazit

Es geht nicht um iT…

Es geht nicht um iT.

Es geht um Ihr Lebenswerk!

Jahrzehnte Aufbau – ggf. bald im Visier.

Noch ist Zeit. Aber nicht ewig.

© R.iT GmbH, 2026

Drei Sätze zum Mitnehmen

1. Für Sie Zufall. Für die Täter Fließbandarbeit.
2. Das Gefährlichste ist nicht die Lücke.
   Es ist der Glaube, keine zu haben.
3. Wer nicht unter NIS-2 fällt, steht auf der Tageskarte.

© R.iT GmbH, 2026

Die letzte leichte Beute

Die Angreifer suchen nicht Sie. Sie suchen offene Türen.
Ob Ihre dazugehört, entscheiden Sie.
Und damit auch, ob Sie die letzte leichte Beute sind.

© R.iT GmbH, 2026

Kurzvorstellung: Tobias Rademann

- Gesellschafter & Geschäftsführer R.iT GmbH (seit 2001)
- Ehrenamt:
  - EU AI Act Advisory Forum
  - Mitglied DIHK IKT-Ausschuss
  - Digitalausschuss IHK Regensburg
- Autor „iT-Due Diligence im Mittelstand” (Springer Gabler, 2026)
- Vorträge und Fachbeiträge zu Digitaler Transformation mit dem Fokus auf Strategie, iT-Sicherheit und KI
- Jahrgang 1972, Wirtschaftswissenschaften & Anglistik (RUB)

© R.iT GmbH, 2026

Die R.iT GmbH – Elevator Pitch

Wir sind eine iT-Unternehmensberatung für den Mittelstand.

Seit über 25 Jahren machen wir erfolgreiche Unternehmen fit für die digitale Zukunft – und damit noch erfolgreicher.

Dafür tun wir drei Dinge:

1. **Wir klären gemeinsam mit der GF die strategische Richtung:**
   Was bedeuten Digitalisierung und KI für Arbeitsweise und Geschäftsmodell?
2. **Wir optimieren Prozesse und iT:**
   Was heute aufhält, läuft morgen – automatisiert, sicher und passgenau.
3. **Wir bewerten iT:**
   Wie viel Zukunft steckt drin, wo sind die Risiken, was ist sie wert?

So stärken wir die Zukunfts- und Wettbewerbsfähigkeit unserer Kunden – und machen den Wert sichtbar, der dabei entsteht.

© R.iT GmbH, 2026

Vielen Dank für
Ihre Zeit und Ihre Aufmerksamkeit!

R.iT GmbH • www.RiT.de

Tobias Rademann, M.A.
Tobias.Rademann@R.iT.de
linkedin.com/in/tobias-rademann-rit/

Vortragsfolien: rit.de/infocenter/vortraege

© R.iT GmbH, 2026