# CYBER RESILIENZ

Wie Unternehmen widerstandsfähig
gegen Cyberangriffe werden

The Matrix has you.

NACH DEM TRAILER

# Willkommen in der Wirklichkeit.

**Aber: Die Grenzen verschwimmen.**

Deep Fakes. KI-gestützte Angriffe.

Automatisierte Manipulation.

> **KI hat in unserer Welt seit ein paar Wochen einen noch stärkeren Einfluss.**

# Cyber Resilienz heißt:

erkennen, reagieren, anpassen – bevor es kritisch wird.

**Hans Otto Mohr**

Development Security
Solutions & Services

**Marco Barth**

Chief Information Security Officer

IT-HAUS GmbH

4 FRAGEN

# Bitte um Handzeichen

IT-HAUS

01 Wer hat heute schon eine KI genutzt?

02 Wer weiß konkret, was mit diesen Daten passiert ist?

03 Wer hat in seinem Unternehmen einen Notfallplan für einen Cyberangriff?

04 Wer hat diesen Plan in den letzten 12 Monaten getestet?

CYBERRESILIENZ

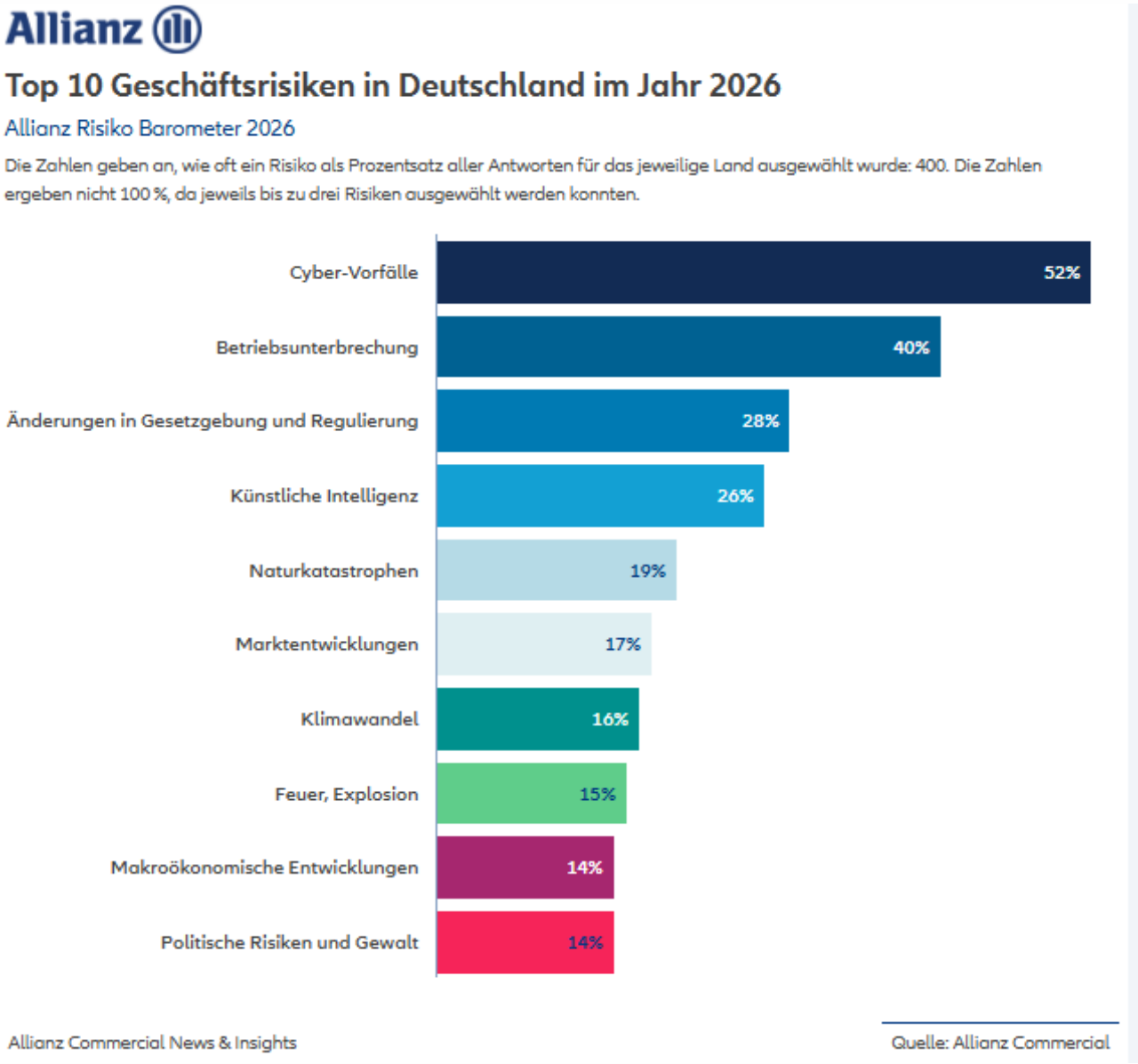
# Nicht perfekte Prävention. Widerstandsfähigkeit.

| 01 | 02 | 03 | 04 | 05 |
|---|---|---|---|---|
| **Vorbereiten** | **Abwehren** | **Reagieren** | **Wiederherstellen** | **Standhalten** |
| Risiken, Szenarien, Rollen | Schutzmaßnahmen & Monitoring | Incident Response | Backups & Wiederanlauf | Widerstandsfähigkeit als Ziel |

*Das Ziel ist nicht, unverwundbar zu sein. Das Ziel ist, handlungsfähig zu bleiben.*

# Das größte Risiko für Unternehmen:

# CYBERVORFÄLLE

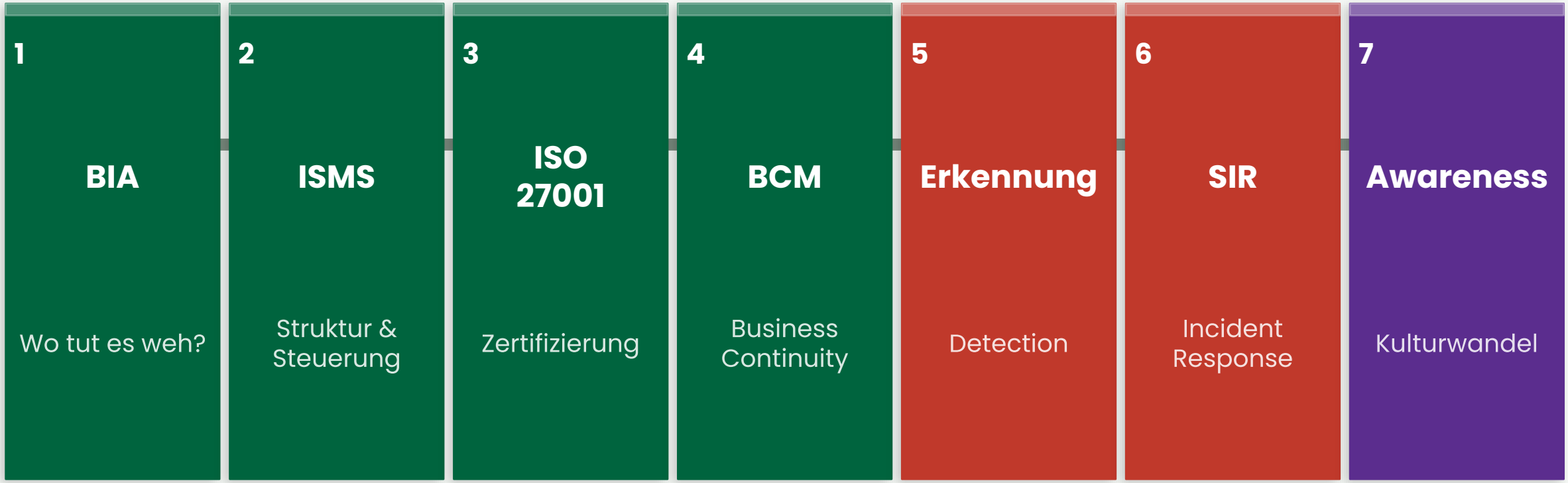


IT-HAUS

*wie haben wir bei IT-HAUS praktisch für Resilienz gesorgt?*

DER WEG

# Resilienz baut man. Schicht für Schicht.



FUNDAMENT

# Wer nicht weiß, was er schützen muss, kann nicht schützen.

## BIA

### Business Impact Analyse

- Was ist kritisch?
- Was kostet ein Ausfall?
- Welcher Schaden tritt ein?

Erst die Antwort auf diese Fragen macht Schutzmaßnahmen sinnvoll. Ohne BIA schützt man alles – und damit nichts.

## ISMS

### Informationssicherheits-Management

- ✓ Sicherheit ist kein Projekt.
- ✓ Sie ist ein dauerhafter Prozess.

Das ISMS liefert euch Struktur, Steuerung und Verantwortlichkeit.

## ISO 27001

### Zertifizierung

- ✓ Kein Selbstzweck – sondern externer Beweis.
- ✓ Kunden, Partner und Behörden wollen Sicherheit sehen.
- ✓ ISO 27001 macht sie messbar.

BETRIEB & REAKTION

# Der Ernstfall kommt. Die Frage ist, ob man bereit ist.

## BCM

### Business Continuity Management

Was tun, wenn kritische Systeme ausfallen?

Der Plan entscheidet, ob das Unternehmen handlungsfähig bleibt. Oder nicht.

## Erkennung

### Detection & Monitoring

Ein Angriff, den man nicht sieht, kann nicht gestoppt werden.

**MDR, SIEM, Monitoring:**
Die Augen, die nie schlafen.

## SIR

### Security Incident Response

Die ersten 60 Minuten entscheiden alles.
Wer entscheidet?

Wer kommuniziert?

Wer schaltet ab?

Das muss vor dem Incident stehen.

Zwei Begriffe. Ein Ziel. Ein klarer Unterschied.

# BCM vs. Resilienz

## BCM

***Was du dokumentiert hast***

Ein Managementsystem mit Prozessen, Plänen und Strukturen. Es beschreibt, wie eine Organisation mit Ausfällen umgehen soll.

- **Prozesse & Pläne**
- **Zertifizierungen & Audits**
- **Übungen & Dokumentation**
- **Rollen & Eskalationswege**

**BCM ist Mittel.**

## Resilienz

***Was du wirklich kannst***

Eine Eigenschaft. Die Fähigkeit, Störungen zu absorbieren, sich anzupassen und handlungsfähig zu bleiben – auch ohne perfekte Pläne.

- **Störungen absorbieren**
- **Anpassen ohne Panik**
- **Handlungsfähig bleiben**
- **Führung & Kultur in der Krise**

**Resilienz ist Ziel.**

BCM IM MITTELSTAND

# Praktikabel statt perfekt.

## Was BSI-Standards vorschlagen

- ✓ Vollständige Business Impact Analyse mit allen Prozessen
- ✓ Detaillierte Notfallpläne für jeden Bereich
- ✓ Jährliche Audits und Zertifizierungen
- ✓ Umfangreiche Dokumentation aller Maßnahmen
- ✓ Regelmässige Übungen und Simulationen

## Was im Mittelstand funktioniert

- ✓ Top-10-Prozesse identifizieren und schützen
- ✓ Einen Notfallplan – der auch gelesen wird
- ✓ Klare Ansprechpartner für den Ernstfall
- ✓ Einmal jährlich durchspielen – 2 Stunden

**Security Incident = BCM-Notfall. Immer.**

DER UNTERSCHIED

# Notfall mit BCM – und ohne.

## MIT BCM

1. **Incident erkannt**
   Meldung läuft sofort
2. **Notfall aktiviert**
   Plan liegt vor, Team steht
3. **Krisenteam handelt**
   Rollen klar, Entscheidung in Minuten
4. **Kommunikation läuft**
   Intern und extern gesteuert
5. **Wiederherstellung**
   Priorisiert, kontrolliert

**Kontrolliert. Schnell. Nachvollziehbar.**

## OHNE BCM

**Wer macht was?**
Keine Verantwortung klar

**IT überlastet**
Alle rufen gleichzeitig an

**Keine Kommunikation**
Kunde hört nichts

**Entscheidung unklar**
Abschalten oder nicht?

**Stunden vergehen**
Schaden wächst

**Chaotisch. Langsam. Teuer.**

KULTURWANDEL

# Resilienz entsteht im Bewusstsein.

**60%**

der vom Verizon DBIR 2025 untersuchten Breaches involvieren den Faktor Mensch

**91 %**

der deutschen KMU halten ihre IT-Sicherheit für gut – erfüllen aber nur 56 % der Basisanforderungen.

*Keine Firewall schützt gegen den Mitarbeiter, der auf den falschen Link klickt. Awareness ist keine Schulung. Es ist eine Haltung.*

**Awareness-Trainings sind kein Nice-to-have. Sie sind der letzte und wichtigste Schutzwall.**

UNSERE EIGENE STORY

# Wir predigen nicht. Wir leben es.

**230+**
Fälle bearbeitet

*Aus der internen Idee, sich selbst besser zu schützen, ist eine echte Truppe geworden:*
**Cyber Incident Response + Business Incident Response – aus einer Hand.**

🎯

## Täglich angegriffen

Nicht theoretisch. Nicht 'irgendwann'. Jeden Tag. Das schlärft den Blick für das, was wirklich zählt – und macht uns besser als jedes Training.

🚔

## CSI Föhren schlägt zu

Organisierte Kriminalität. Echte Täter. GPS-Ortung. Peilsender. Telefonüberwachung per Gerichtsbeschluss. Spektakuläre Verhaftung. Die Kripo hat sich persönlich bedankt.

🛡️

## Cyber IR

Ransomware. Datenlecks. APT-Angriffe. 230+ Fälle. Echte Einsätze. Kein Lehrbuch. Einsatzbereitschaft ist unser Standard – nicht unser Anspruch.

💼

## Business IR

Fraud. Warenkredit-Betrug. Social Engineering. Resilienz hört nicht an der IT-Grenze auf. Wir sichern den Betrieb – nicht nur die Systeme.

*Kein Hersteller hat angerufen.* ***Was uns gerettet hat: Meldekette, Entscheidung, Handlung. Nicht die Firewall.***

MDR ist der Sensor.

# IT-HAUS IR das Krisenteam.

## MDR — Managed Detection & Response

*z.B. Sophos MDR, Watchguard, Crowdstrike, andere Anbieter*

- 24/7 Monitoring aller ongeboardeten Systeme — KI-gestützt, durch Experten validiert
- Erkennung & Einordnung von Anomalien und Bedrohungen inkl. Root-Cause Analyse
- Automatisches Containment bei erkannten Angriffen
- Liefert konkrete Handlungsempfehlungen an den Kunden

⚠ Endet nach Containment — kein Wiederanlauf, keine Managementkommunikation, keine Drittparteien

+

## IT-HAUS Incident Response

*Notfall- & Krisenteam — End-to-End, ein Ansprechpartner*

- Gesamter IR-Lebenszyklus: Vorbereitung bis Nachbereitung
- Krisenkommunikation: Vorlagen, Management, Eskalation
- Infrastruktur-Wiederanlauf (Citrix, MS, Netzwerk, Firewall)
- Forensik, Bereinigung & Begleitung bei DSB, LKA, BSI

✓ Aktivierbar Ad-hoc oder via Retainer — schnell, planbar, priorisiert. Ein Team, ein Vorgehen.

**IR-PHASEN ABDECKUNG**




Produktinformation: Cyber Notfallhilfe (Ad-hoc) & Incident Response Retainer

# Cyber Notfallmanagement

Von Prävention bis Notfallhilfe – IT-Security für jedes Unternehmen

IT-HAUS

⚠️

### Akuter Sicherheitsvorfall?

Wir stoppen die Ausbreitung, schaffen Klarheit und bringen Sie mit Security Incident Response schnell zurück in den Betrieb.

Vorfall melden

💡

### Vorbereitet statt überrascht

Mit Cyber-Notfallvorsorge kennen und überwachen wir Ihre Systeme, haben mit Ihnen geübt und reagieren im Ernstfall sofort – garantiert.

Mehr erfahren

# Security Incident Response Services

IT-HAUS

| Feature | Cyber-Notfallhilfe | Cyber-Notfallvorsorge | | |
|---|---|---|---|---|
| | Ad-hoc | Basic | Pro | Premium |
| Erstreaktion | Best Effort | <4h | <2h | <1h |
| Servicezeit | Best Effort | Mo–Fr 08–17 Uhr | Mo–Fr 08–20 Uhr | 24/7 |
| Hotline | ✓ | ✓ | ✓ | ✓ |
| Web-Notfallmeldung | ✓ | ✓ | ✓ | ✓ |
| Security Incident Manager | ✓ | ✓ | ✓ | ✓ |
| Onboarding | – | ✓ | ✓ | ✓ |
| Reporting / Review | – | jährlich | halbjährlich | halbjährlich |
| Kundenspezifische Playbooks | – | optional | ✓ | ✓ |
| Notfallübungen | – | optional | jährlich | halbjährlich |
| Vor-Ort Einsatz | optional | optional | ✓ | ✓ |

# Leistungsumfang Notfallhilfe

**Analyse von laufenden Sicherheitsvorfällen**
→ Identifikation von Ursache, Umfang und Kritikalität

**Umsetzung von Sofortmaßnahmen und Eindämmung**
→ Wir sorgen dafür, dass ein Angriff gestoppt wird und sich nicht weiter ausbreitet

**Forensik, Handlungsempfehlungen & sicherer Wiederanlauf**
→ Erstellung von Berichten und Empfehlungen zur Verbesserung der IT-Sicherheit
→ Wir helfen Kunden dabei wieder handlungsfähig zu werden
→ Erstellung eines umfassenden Abschlussberichts zum Vorfall

**Krisenkoordination, -Kommunikation und -Reaktion:**
→ Unterstützung bei der internen und externen Kommunikation, bspw. mit Behörden oder betroffenen Parteien

UNSER ANGEBOT

# Von Prävention bis Krisenreaktion.

## 📋 BCM & Notfallmanagement

Beratung, Strukturaufbau, Notfallpläne – praxistauglich für den Mittelstand.

## 🔍 Security Checks

Status Security, Backup-Check, Entra-ID, Prüfung technischer Systeme.

## 🎯 Notfallübungen

Table Top Excercise und Simulationen – damit der Plan im Ernstfall sitzt.

## 🧠 Awareness Training

Schulungen, Phishing-Simulationen, Kulturwandel als Dauerprozess.

## 👁️ Managed Detection & Response

24/7 KI-gestütztes Monitoring. Erkennung, Einordnung, Containment.

## 🚨 Security Incident Response

End-to-End Krisenteam. Von der ersten Minute bis zum Wiederanlauf.

**I IT-HAUS – Ihr Partner. Vom ersten Check bis zur Krisenbewältigung.**

IT-HAUS

“

***Was wäre der eine konkrete Schritt, den ihr morgen in eurem Unternehmen anstoßen könntet?***

5 TIPPS

# Was ihr morgen früh umsetzen könnt.

IT-HAUS

**01**

## Jeden Security Incident als BCM-Notfall behandeln.

Nicht erst ab Stufe Critical. Sofort. Notfallplan aktivieren, Krisenteam einbeziehen. Lieber einmal zu viel als einmal zu spät.

**02**

## Top 10 kritische Prozesse benennen – heute.

Was darf unter keinen Umständen ausfallen? Wer das nicht beantworten kann, schützt das Falsche.

**03**

## BCM schlank halten – kein BSI-Vollprogramm

Ein Plan, der gelesen wird, ist besser als 200 Seiten Dokumentation, die niemand kennt.

**04**

## Entscheidungsbaum für den Ernstfall definieren.

Wer darf abschalten? Wer kommuniziert nach außen? Schreibt es auf ein DIN-A4-Blatt. Hängt es auf.

**05**

## Einmal jährlich üben. Zwei Stunden reichen.

Notfallübung im Team: Was tun wir, wenn morgen früh der Alarm losgeht? Die Antworten werden euch überraschen.

3 THESEN

# Merkt sie euch. Ihr werdet sie heute noch brauchen.

**01**

**Angreifer suchen keine Lücken. Sie suchen fehlende Entscheidungen.**

*Jeder Angriff, den ihr heute Nachmittag seht, hat einen menschlichen Entscheidungsmangel als Grundlage.*

**02**

**Der gefährlichste Moment ist nicht der Angriff. Es ist die erste Stunde danach.**

*Immanuel Bär zeigt euch den Einbruch. Fragt euch: Was passiert danach in eurer Organisation?*

**03**

**Cyber Resilienz ist kein IT-Thema. Es ist eine Führungsentscheidung.**

*Wer das dem IT-Team allein überlässt, hat die Verantwortung bereits abgegeben.*

IT-HAUS

# Er zeigt euch, wie Angreifer arbeiten.

*Ich bitte euch um eines:*

## Schaut nicht auf die Technik.

*Fragt euch bei jedem Angriff, den er zeigt:*

**Welche unserer drei Thesen hätte das verhindert?**

IT-HAUS

DIE LAGE

# Warum jetzt. Warum jeder.

## #1

## Cyber-Risiko

ist laut Allianz Risk Barometer 2026 das größte Geschäftsrisiko weltweit.
Nicht Inflation. Nicht Lieferketten. Cyber.

Allianz Risk Barometer 2025

## KI

## als Angriffsbeschleuniger

KI demokratisiert das Hacking. Was früher Expertise brauchte, braucht heute einen Prompt.

Der Angreifer von heute hat Ressourcen, Geduld und politische Deckung.

# Was wir leisten können

## 1. Starterpaket Notfallmanagement (Festpreis 3.500 €)

**1**

**Vorbereitung**

- ✓ Kick-Off-Meeting
- ✓ Vorab-Fragebogen
- ✓ Reifegradanalyse in Bezug auf IT-Notfallmanagement

**2**

**Workshop**

- ✓ Überblick über Begrifflichkeiten
- ✓ Vorstellung der Ergebnisse der Reifegradanalyse
- ✓ Bereitstellung der Vorlagen
- ✓ Erarbeitung der nächsten Schritte

**3**

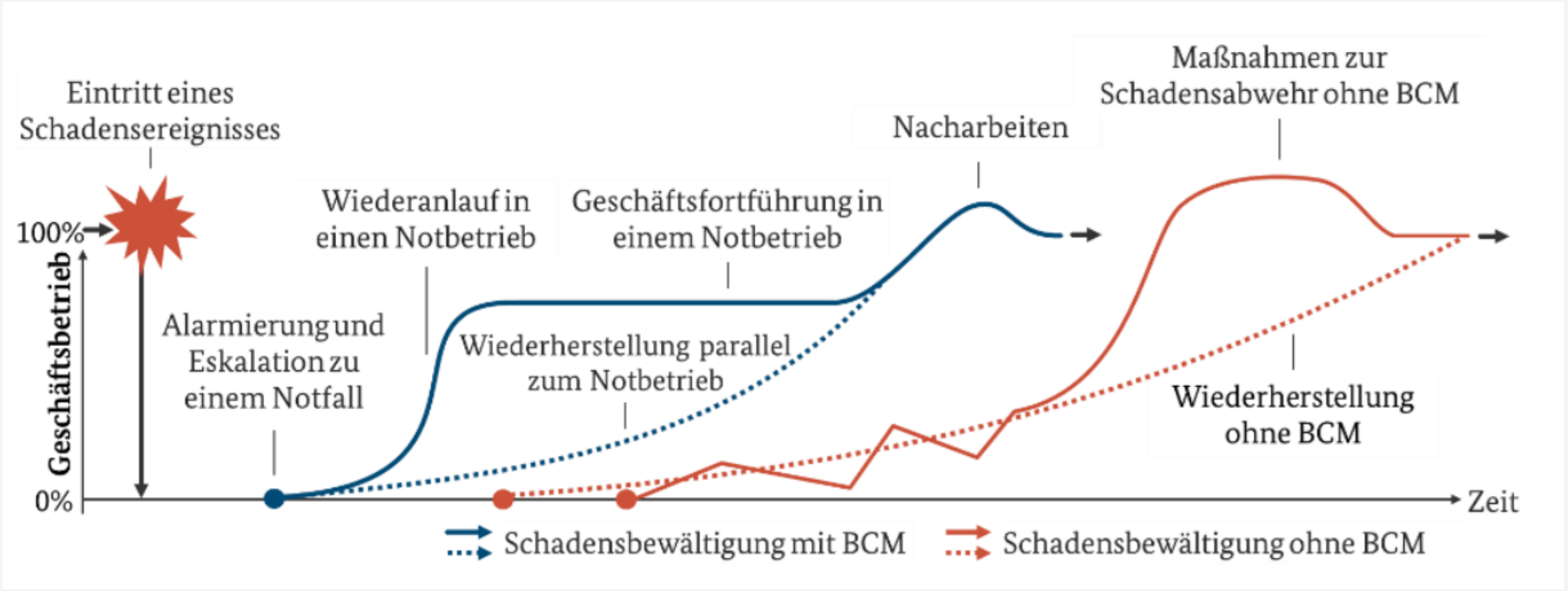
**Arbeitsphase & Review**

- ✓ selbstständige Bearbeitung durch den Kunden
- ✓ Reviewtermin zur Besprechung der Fortschritte und Fragen
- ✓ Klärung weiterer Unterstützungsbedarf

## 2.Folgedienstleistungen (Abrechnung nach Zeit), bspw.:

- Erarbeitung von spezifischen Szenario-Handbüchern
- Entwicklung einer Melde-App für Notfallalarmierung
- Grundlegende Security Incident Response-Prozesse (bspw. MDR)

# Mit vs. Ohne BCM



Während IT die Wiederherstellung plant – was tun die Fachbereiche? Wer hat eine Antwort?

# Ist Ihr Unternehmen ohne IT überlebensfähig?

## Ohne Vorbereitung

*Das passiert ohne Ersatzbetrieb:*

- Kein Überblick – Telefon regiert
- Entscheidungen ohne Datenbasis
- Manuelle Prozesse ad hoc, fehlerhaft
- Kundenversprechen gebrochen
- Compliance-Risiken (Fristen, Meldungen)
- Führung verliert Kontrolle

## Mit Ersatzbetrieb

*Was Ersatzbetrieb ermöglicht:*

- Fachbereiche bleiben handlungsfähig
- Manuelle Abläufe sind definiert & geübt
- Mindestdaten sind offline verfügbar
- Kritische Fristen werden eingehalten
- Klare Rollen & Eskalationswege
- IT kann sich auf Recovery fokussieren

## Unser Ansatz

*Ersatzbetriebsverfahren pro Fachbereich:*

- RTO-orientiert: HOCH / MITTEL / NORMAL
- Kritikalität je Prozess bewertet
- Konkrete Sofortmaßnahmen definiert
- Mindestdaten & Offline-Ressourcen
- Fristen & Compliance verankert
- Fachbereich-geführt – nicht IT-abhängig

**Ersatzbetrieb ist keine IT-Aufgabe. Es ist Führungsverantwortung – und der Test, ob BCM wirklich gelebt wird.**