THE SPIR.IT OF EXCELLENCE

iT-Sicherheit:
Gordischer Knoten oder Sisyphusarbeit?

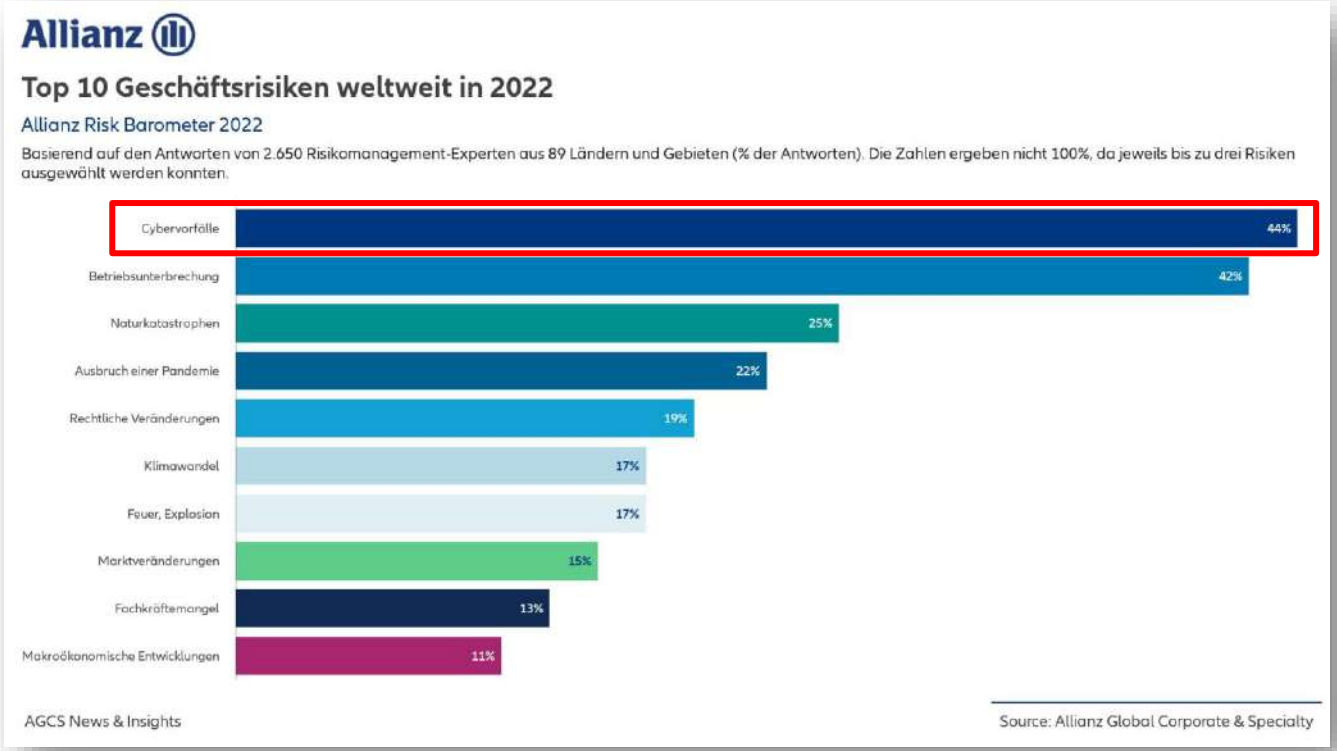
Vortrag im Rahmen der LogCoop Vollversammlung 2022

Tobias Rademann

20. Juni 2022

iT-Sicherheit ist (überlebens-)wichtig

iT-Sicherheit ist (überlebens-)wichtig



oder aber…

Demo: Cyber Angriff 'Erpressungstrojaner'

Anmerkung:

An dieser Stelle wurde im Rahmen des Vortrags ein Video eines Angriffs mit einem Erpressungstrojaner gezeigt.

Das war's!

Ihre Daten sind jetzt *weg.*

Ihre Systeme stehen *still.*

Ihre Mitarbeiter*innen sind *verunsichert.*

Sie sind weder *handlungs*- noch *auskunftsfähig*.

Ihre Kunden bekommen *Angst*.

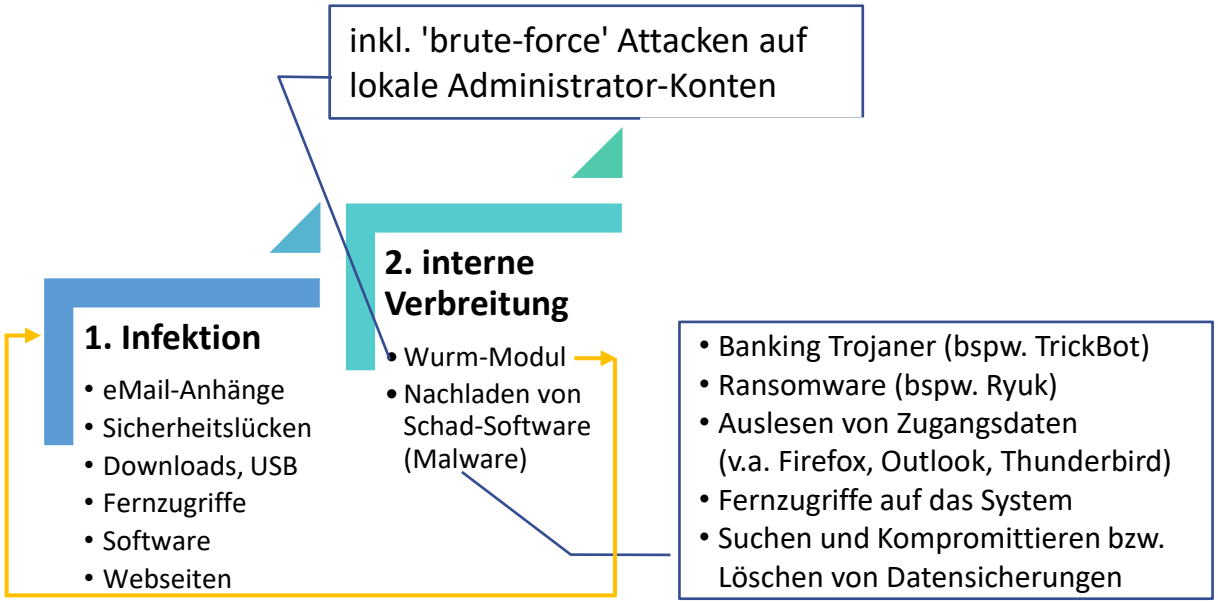
Und wenden sich *ab*.

Viel Geld steht auf dem Spiel.

… und die ***Existenz***
Ihres Unternehmens!

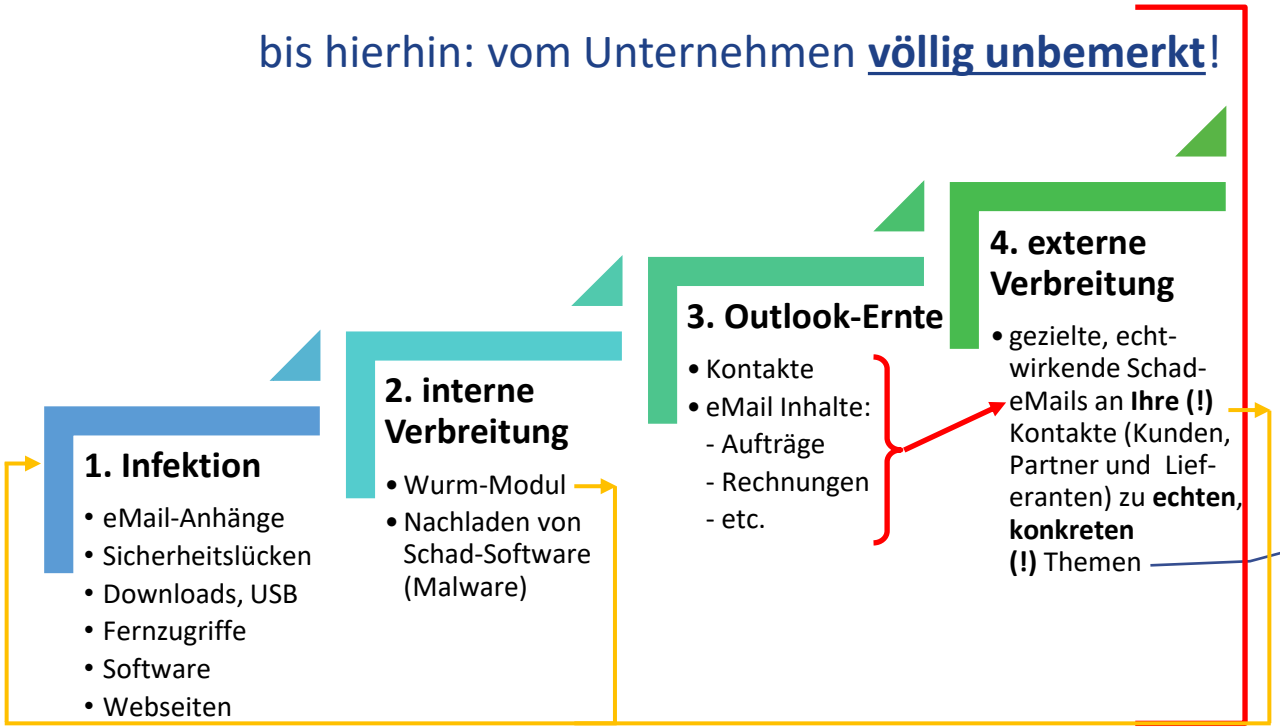
aber dennoch…

Erpressungstrojaner 2.0



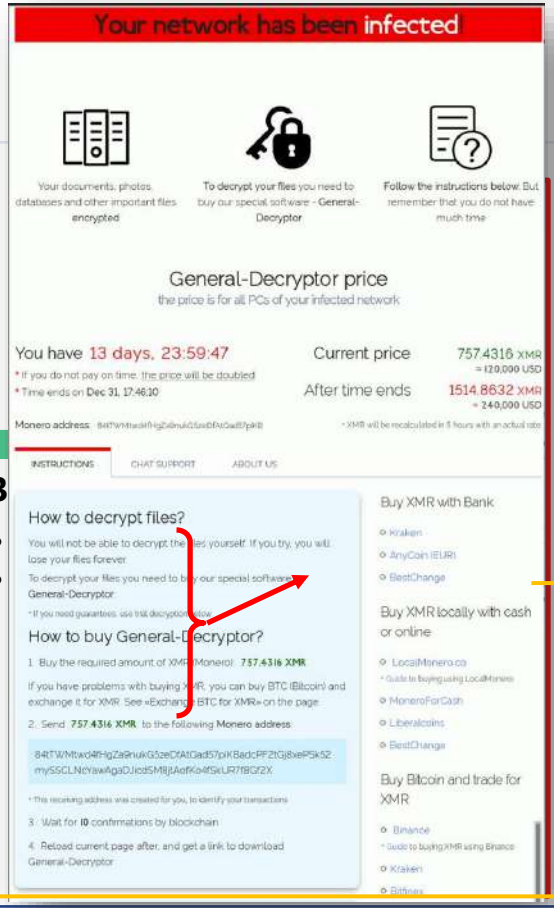
Erpressungstrojaner 2.0

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



BSI (2019):
"die für die Empfänger (künftig) **kaum noch** als solche [Schad-eMails] zu identifizieren sind"

Erpressungstrojaner



1. Infektion

- eMail-Anhänge
- Sicherheitslücken
- Downloads, USB
- Fernzugriffe
- Software
- Webseiten

2. interne Verbreitung

- Wurm-Modul
- Nachladen von Schad-Software (Malware)

3

-
-

5. finaler Schritt

- **Verschlüsseln** Ihrer Daten

6. Erpressung

→ Geld zum **Entschlüsseln** Ihrer Daten

Ergebnis:

- wochenlanger Ausfall
- extrem schmerzhafte finanzielle Schäden
- Reputationsverlust
- …

Die Champions League

lessons learned

Beim Thema iT-Sicherheit geht es um den
Schutz Ihres Unternehmens!

Jetzt. Heute. In diesem Moment.
Für die Zukunft.

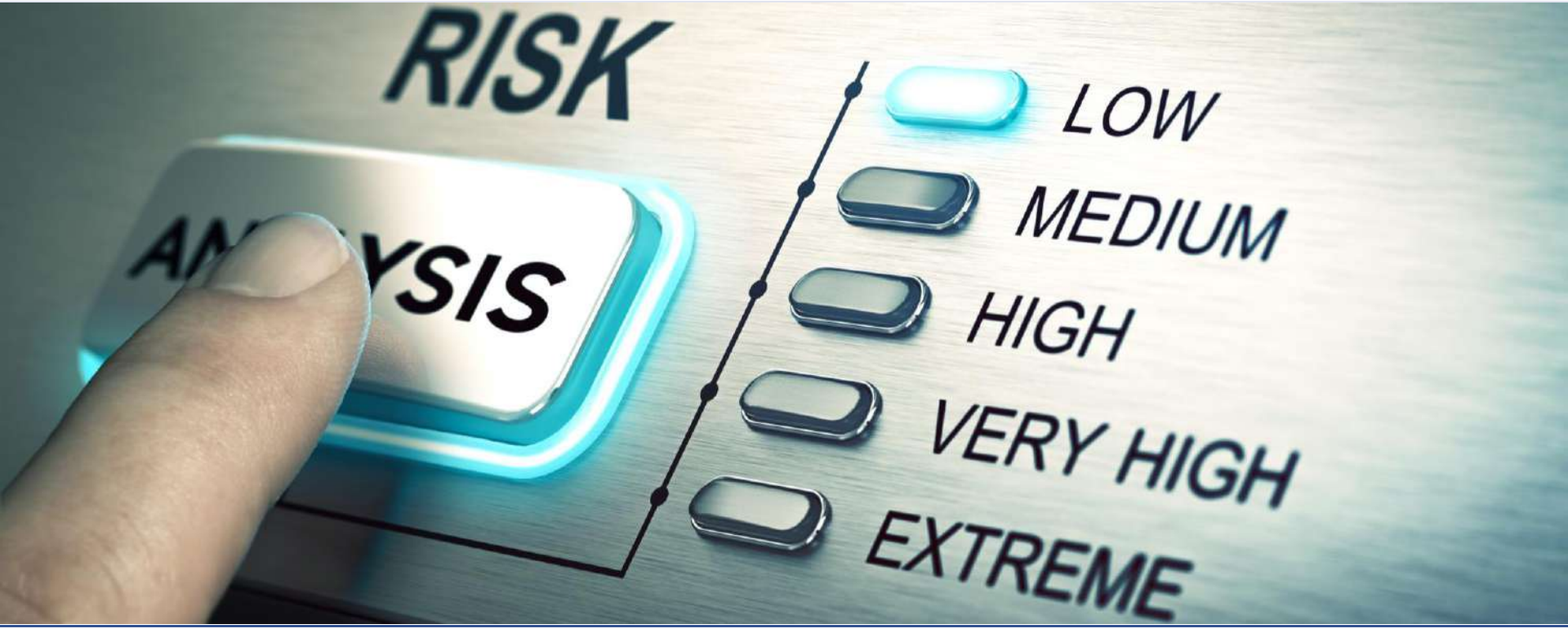
lessons learned

Unternehmensgröße, Kontostand, Branche sind egal.

Cyberkriminelle haben es auf **alle Unternehmen** abgesehen.

lessons learned

lessons learned



lessons learned

nur was?

Die Lösung

behandeln Sie iT-Sicherheit wie jedes andere komplexe Thema

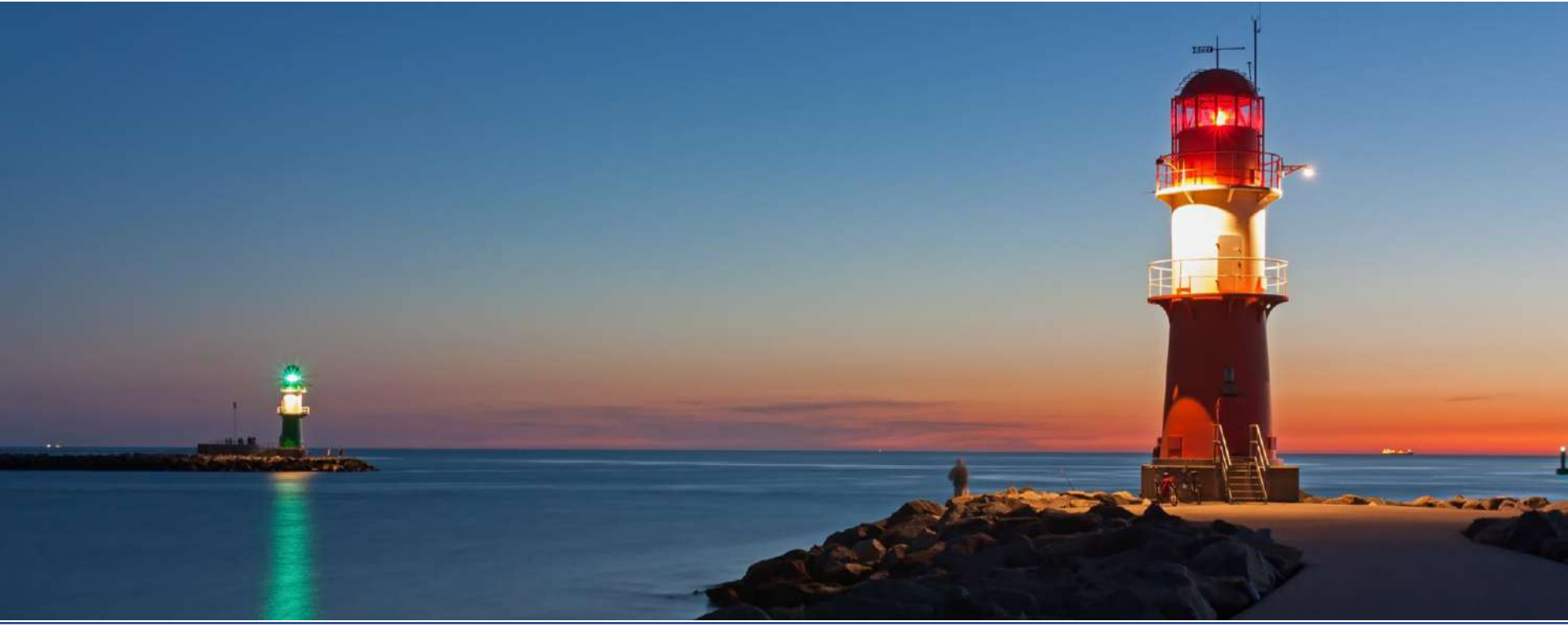
1. Suchen Sie sich einen kompetenten Partner!

1. Suchen Sie sich einen kompetenten Partner!

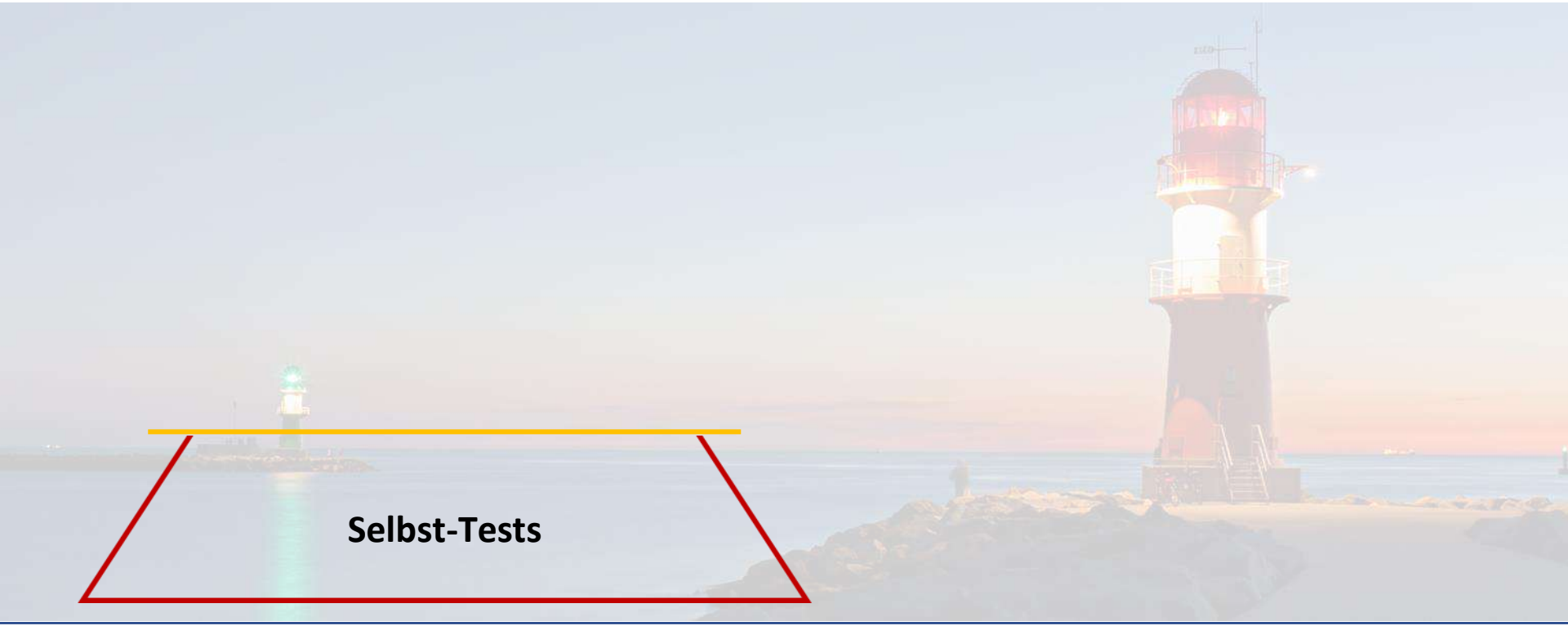
zentrale Eigenschaften

- Schwerpunkt = iT-Sicherheit!
- Erfahrung

2. Verschaffen Sie sich einen Überblick



2. Verschaffen Sie sich einen Überblick



Fall 1

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

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

Fall 2

24.11.: Angebotsbesprechung 'iT Risk Assessment'

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

26.11.: 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 dem 09.11. kompromittiert**.
  Datensicherung: Historie: **nur 1 Woche**
  Umfang: **lückenhaft**; cloud fehlte **vollständig**

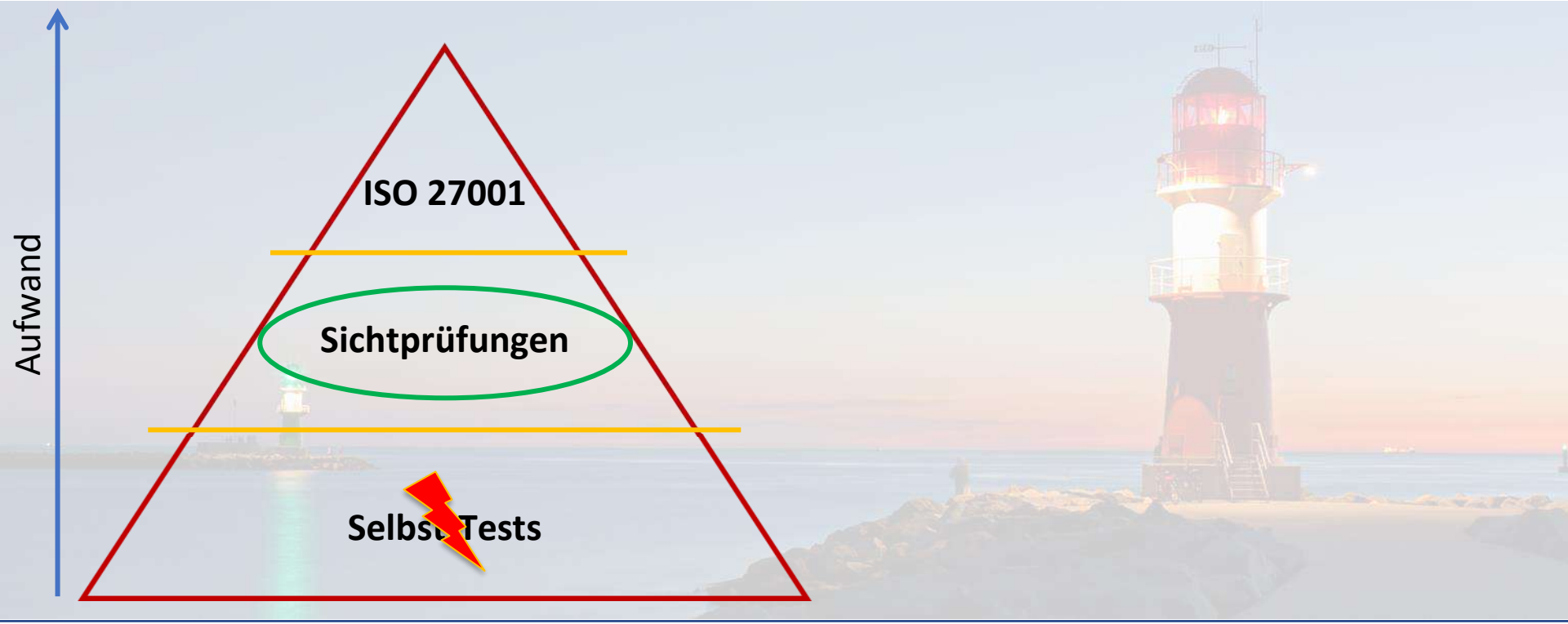
2. Verschaffen Sie sich einen Überblick

Warum Sichtprüfungen?

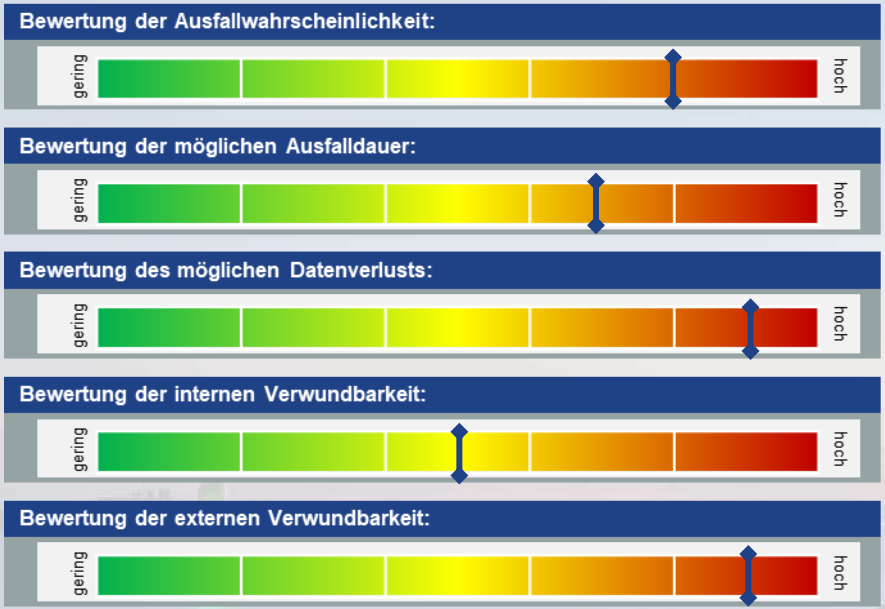
Bei iT-Sicherheit macht niemand (!)
absichtlich und *bewusst* etwas falsch!

→ Gründe für Fehler: fehlendes Wissen / Erfahrung, Flüchtigkeitsfehler

2. Verschaffen Sie sich einen Überblick



Das RIT® iT-Risk Assessment

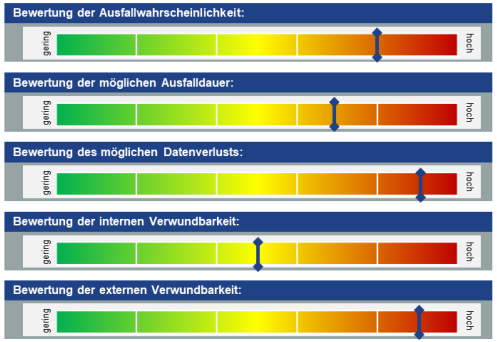


CYBERSECURITY MADE IN EUROPE™

Initiated by ECSO. Issued by eurobits e.V.

Vorteile Sichtprüfung

- ✓ fundierte Ergebnisse
- ✓ Bewertung der 5 zentralen Risiken
- ✓ objektiv(er) durch externen Sicht
- ✓ nicht-invasiv
- ✓ checklistenbasiert
- ✓ i.d.R. viele Jahre Erfahrung



CYBERSECURITY™
MADE IN EUROPE

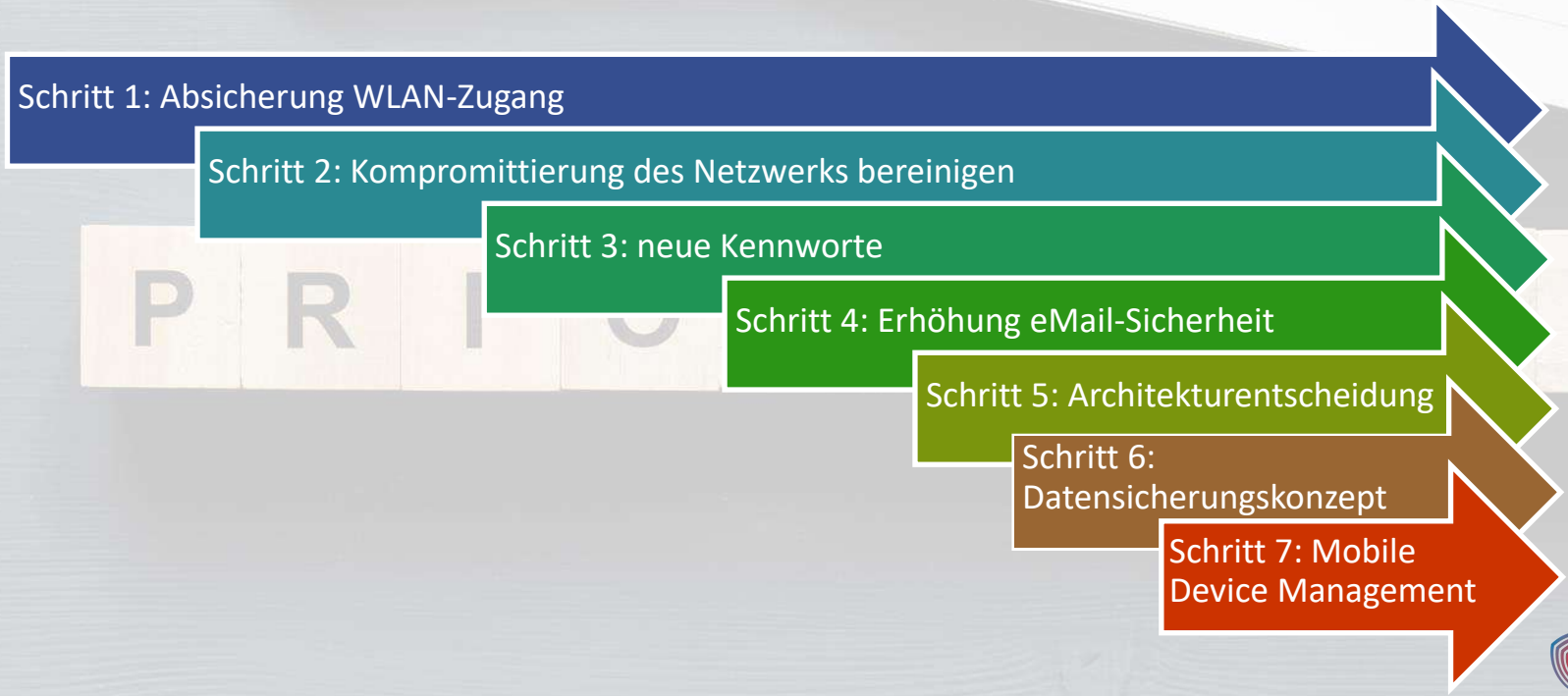
Initiated by ECSO. Issued by eurobits e.V.

Das RIT® iT-Risk Assessment

Ablauf

3. priorisieren Sie die To Dos (nach Hebel!)

3. bewerten / priorisieren Sie die To Dos



CYBERSECURITY MADE IN EUROPE

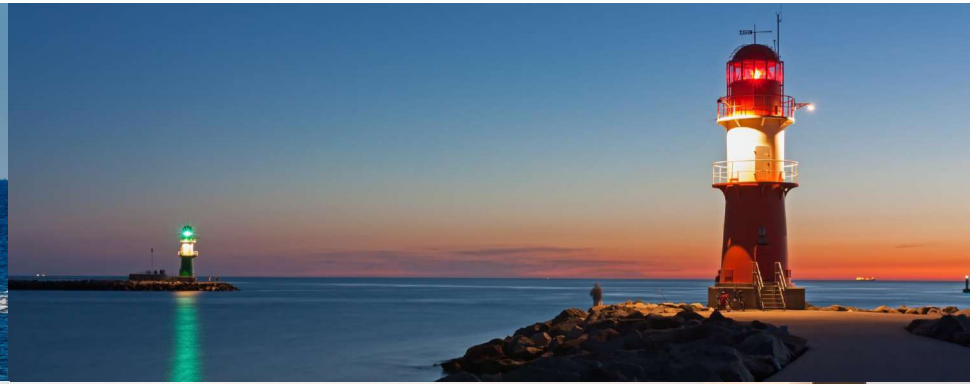
Initiated by ECSO. Issued by eurobits e.V.

4. beginnen Sie mit der Umsetzung

4. beginnen Sie mit der Umsetzung

- ✓ in Abstimmung mit Ihrem Budget (Zeit & Geld)
- ✓ schrittweise & regelmäßige Umsetzung der nächst-priorisierten Maßnahme

Vorgehen



Résumé

Gordischer Knoten?

= die Überwindung eines **schwierigen Problems** mit **unkonventionellen** Mitteln

nein, denn:

- iT-Sicherheit ist zwar komplex
- aber 'konventionelle' Mittel führen zum Ziel:
  - ✓ Überblick verschaffen
  - ✓ strukturiertes und priorisiertes Vorgehen
  - ✓ Standardwerkzeuge und -methoden

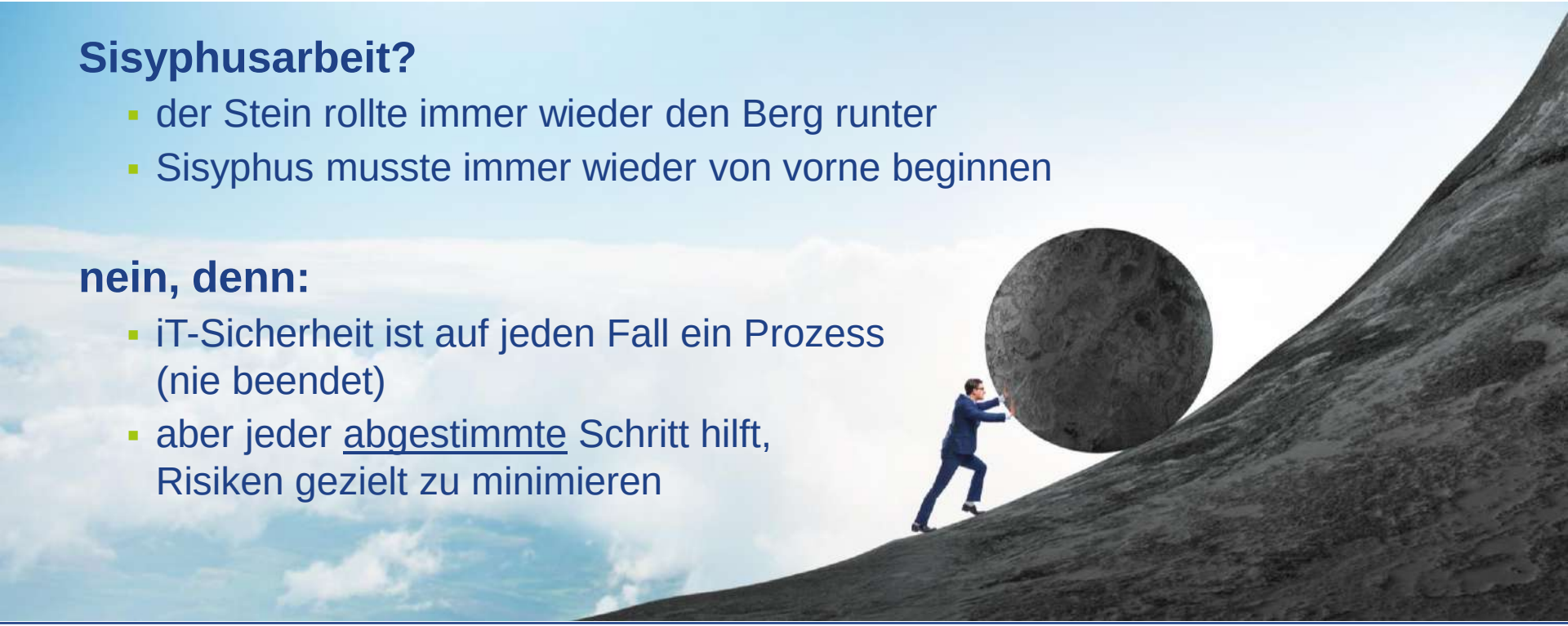
Résumé

Sisyphusarbeit?

- der Stein rollte immer wieder den Berg runter
- Sisyphus musste immer wieder von vorne beginnen

nein, denn:

- iT-Sicherheit ist auf jeden Fall ein Prozess (nie beendet)
- aber jeder abgestimmte Schritt hilft, Risiken gezielt zu minimieren



Résumé

Also: Legen Sie los & schützen Sie Ihre Unternehmen und deren Zukunft!

offene Fragen / Diskussion

Vielen Dank für
Ihre Zeit und Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:

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

Tobias Rademann, M.A.
R.iT GmbH • www.RiT.de
Zentrale: Lise-Meitner-Allee 37, 44801 Bochum
Tel.: (0234) 43 88 00-0, Fax: -29
NL Nord: Tremskamp 5, 23611 Bad Schwartau
Tel.: (0451) 203 68-500, Fax: -499
eMail: Tobias.Rademann@RiT.de

Kurzprofil: R.iT GmbH

- **Ausrichtung:** iT-Unternehmensberatung
- **Fokus:** Digitale Transformation Ihres Unternehmens
  > Strategie
  > Organisation
  > Informationstechnologie

  → **Chancen** nutzen!
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte** Zentrale: Bochum
  Region Nord: Bad Schwartau
- **Zertifizierung:** BMWi-autorisiert für > iT-Sicherheit *und*
  > digitale Geschäftsprozesse
  Deutscher Excellence Preis 2021 in Bronze

go-digital

DEUTSCHER EXCELLENCE PREIS 2021 BRONZE

hilfreiche Quellen:

- "**100.000 Euro für Ihre Daten?**"; Air Truck Service GmbH / R.iT GmbH; https://www.rit.de/success-stories/ats-air-truck-service-gmbh-it-sicherheit
- **"IT-Sicherheit im Home-Office im Jahr 2020"**; Bundesamt für Sicherheit in der Informationstechnologie; https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html
- **"The rise of ransomware during COVID-19 – How to adapt to the new threat environment."**; Ferbrache, David (KPMG); https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html
- **"iT-Sicherheit zu Zeiten von Corona: Erfahrungsbericht aus dem ‘new normal’"**; Rademann, Tobias (R.iT); https://www.rit.de/unternehmen/downloads/vortraege