



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



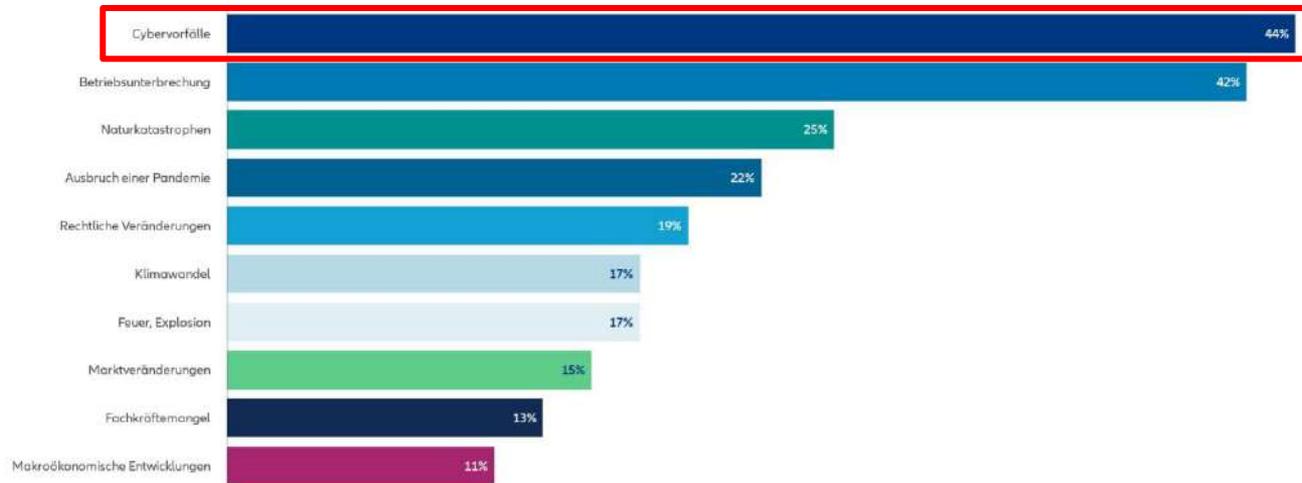
# iT-Sicherheit ist (überlebens-)wichtig



## Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Source: Allianz Global Corporate & Specialty

*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*.

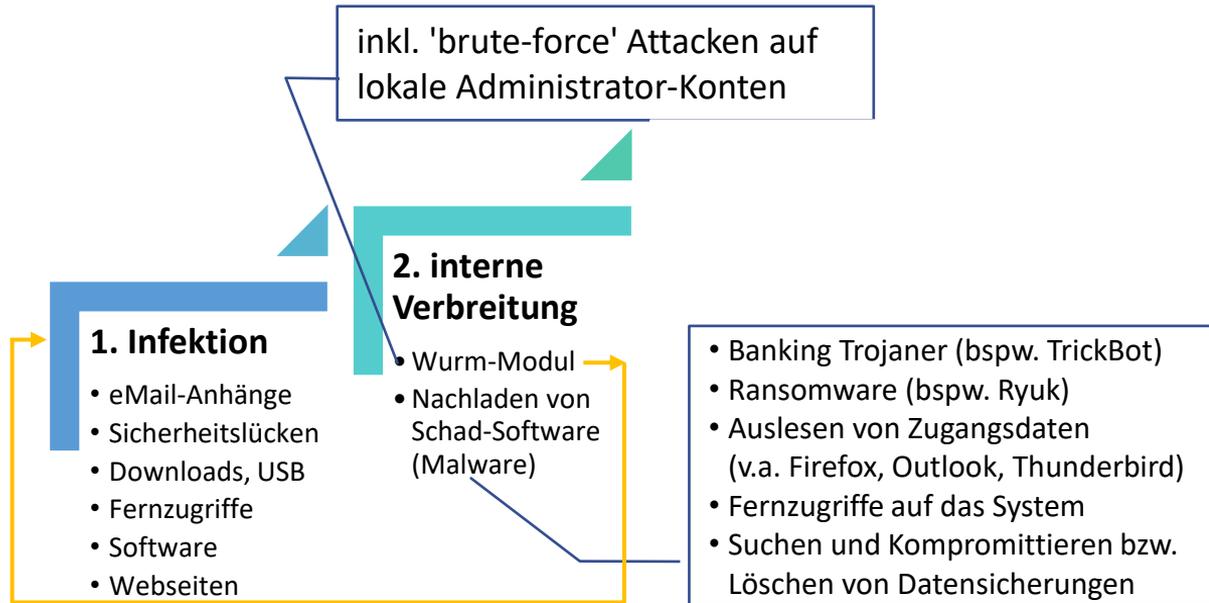
Viel Geld steht auf  
dem Spiel.

... und die *Existenz*,  
Ihres Unternehmens!

*aber dennoch...*

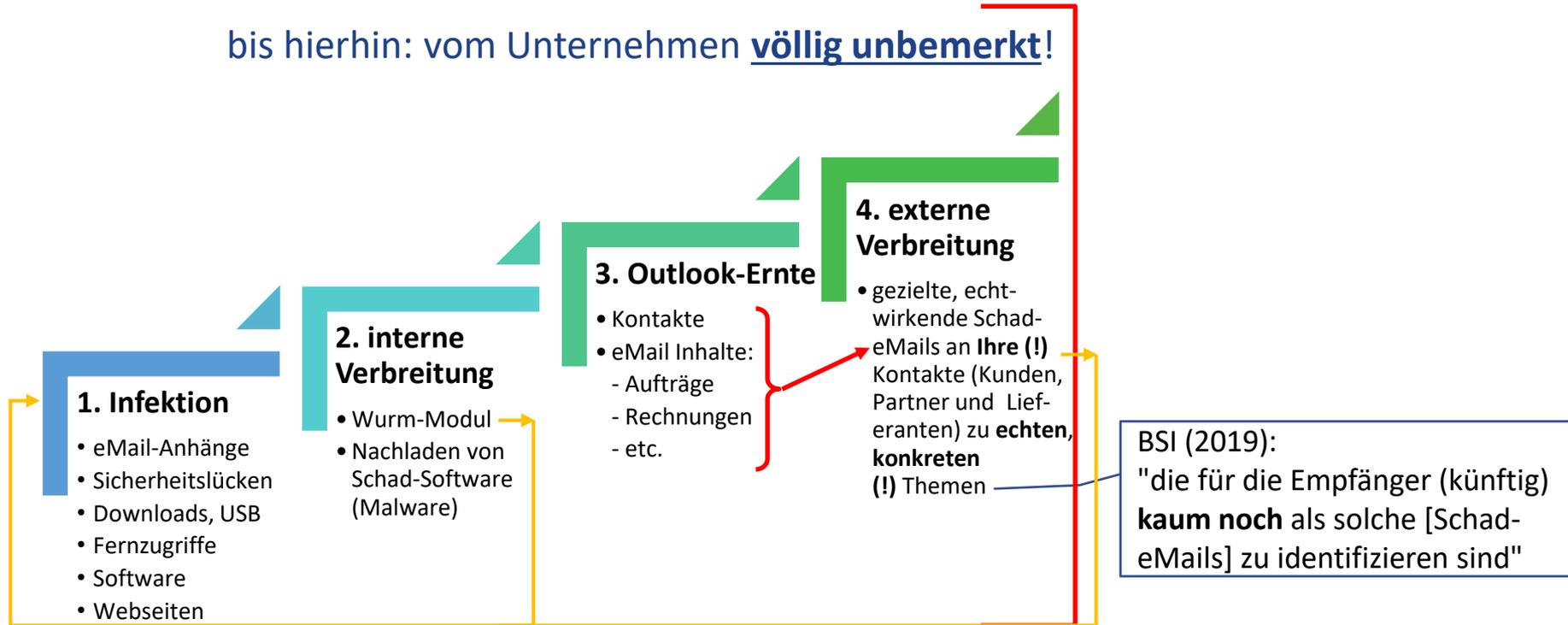
A colorful logo for 'KINDERGARTEN'. The word is written in large, bold, multi-colored letters. Above the letter 'I' is a yellow sun with a smiling face and rays. The colors of the letters are: K (orange), I (yellow), N (red), D (blue), E (green), R (purple), G (red), A (orange), R (yellow), T (green), E (blue), N (purple).

# Erpressungstrojaner 2.0

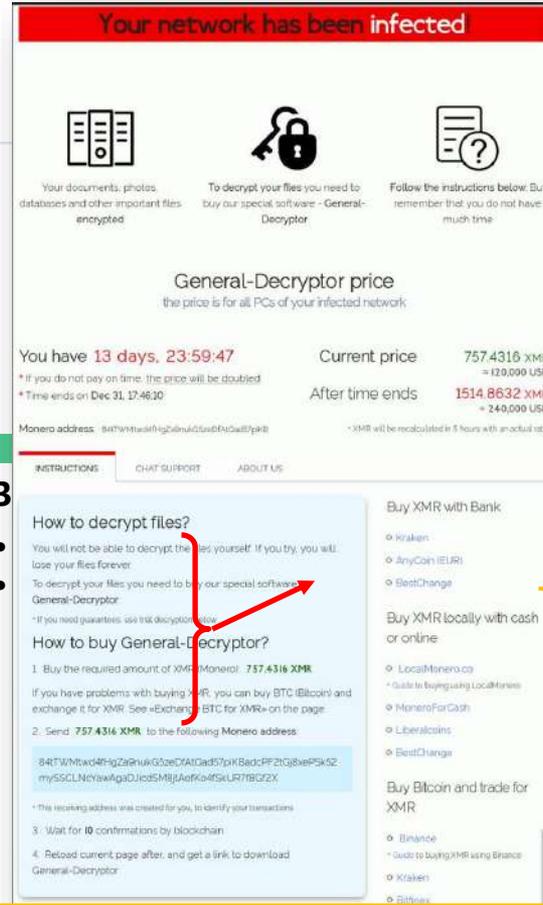


# Erpressungstrojaner 2.0

bis hierhin: vom Unternehmen völlig unbemerkt!



# 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 schmerzhaft finanzielle Schäden
- Reputationsverlust
- ...

# Die Champions League



A top-down view of a dark grey chalkboard. In the top left corner is a white coffee cup with a saucer containing dark coffee. In the top right corner is a white pen. In the bottom right corner is a magnifying glass with a black handle. The words 'LESSONS LEARNED' are written in the center in white chalk, arranged in two lines: 'LESSONS' on top and 'LEARNED' on the bottom. The magnifying glass is positioned over the end of the word 'LEARNED'.

## 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



Gelegenheit macht  
Diebe.

# lessons learned



# lessons learned

**do it now**

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

A background image showing a lighthouse on a rocky island at sea during sunset or sunrise. The sky is a mix of orange, pink, and blue. The lighthouse is illuminated from within, casting a warm glow. In the distance, another smaller lighthouse is visible on the horizon.

**Selbst-Tests**

# 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

The background of the slide is a photograph of a lighthouse on a rocky island at sea during sunset or sunrise. The sky is a mix of orange, pink, and blue. The lighthouse is a tall, cylindrical structure with a lantern room at the top. A smaller lighthouse is visible in the distance on the left.

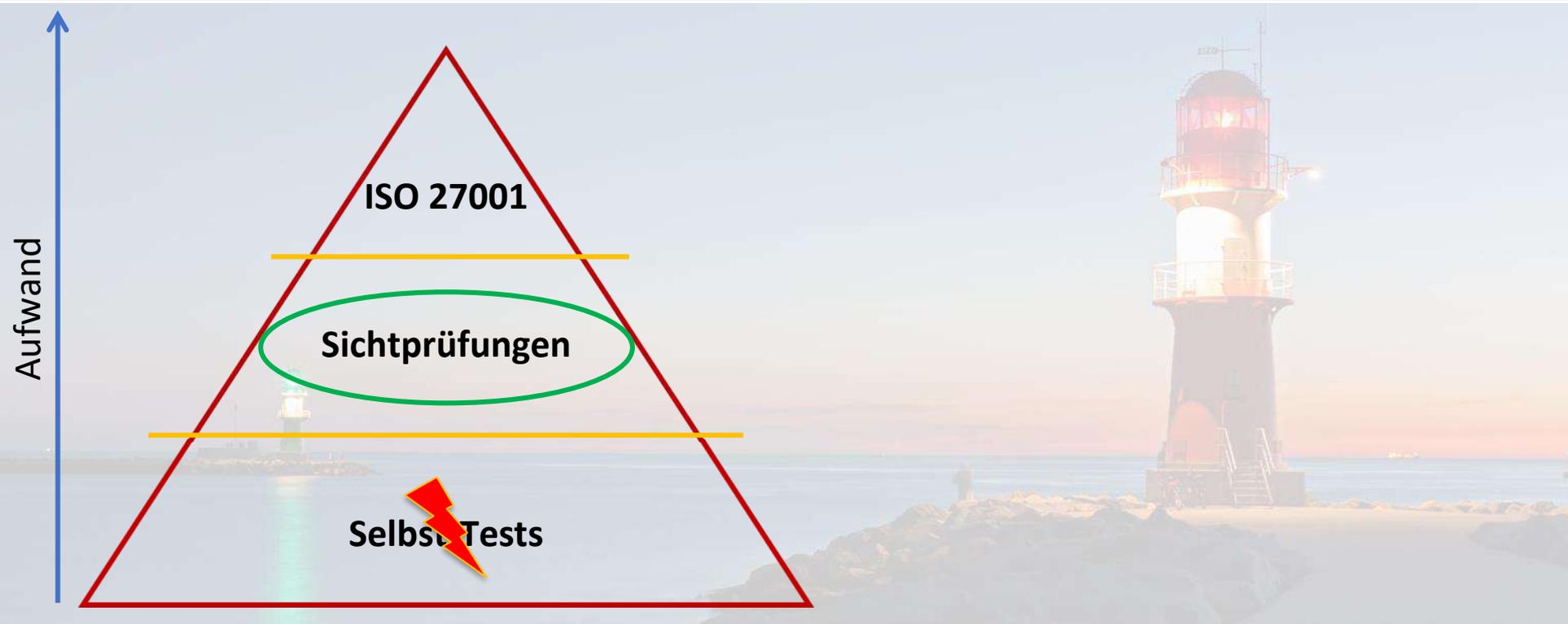
**Selbst Tests**

# Warum Sichtprüfungen?

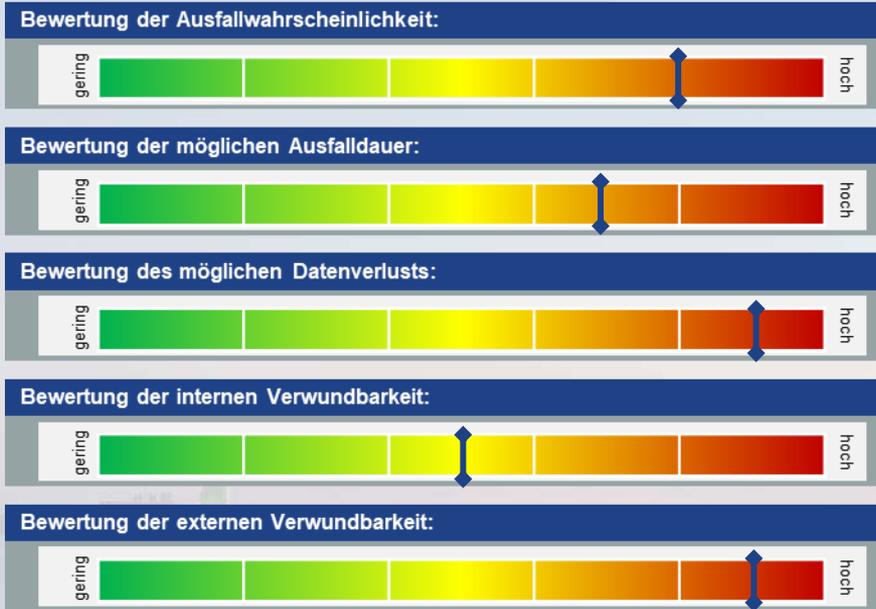
Bei iT-Sicherheit macht niemand (!)  
*absichtlich* und *bewusst* etwas falsch!

→ Gründe für Fehler: fehlendes Wissen / Erfahrung, Flüchtigkeitsfehler

## 2. Verschaffen Sie sich einen Überblick



# Das RIT<sup>®</sup> iT-Risk Assessment

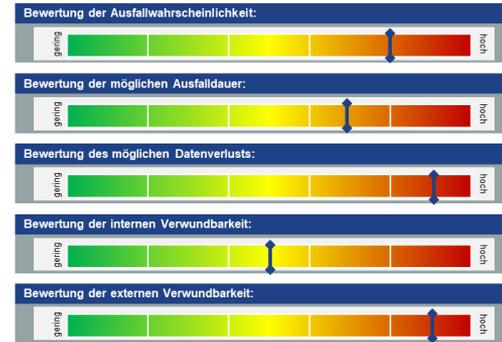


CYBERSECURITY<sup>TM</sup>  
MADE IN EUROPE

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<sup>TM</sup>  
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

# Das RIT<sup>®</sup> iT-Risk Assessment

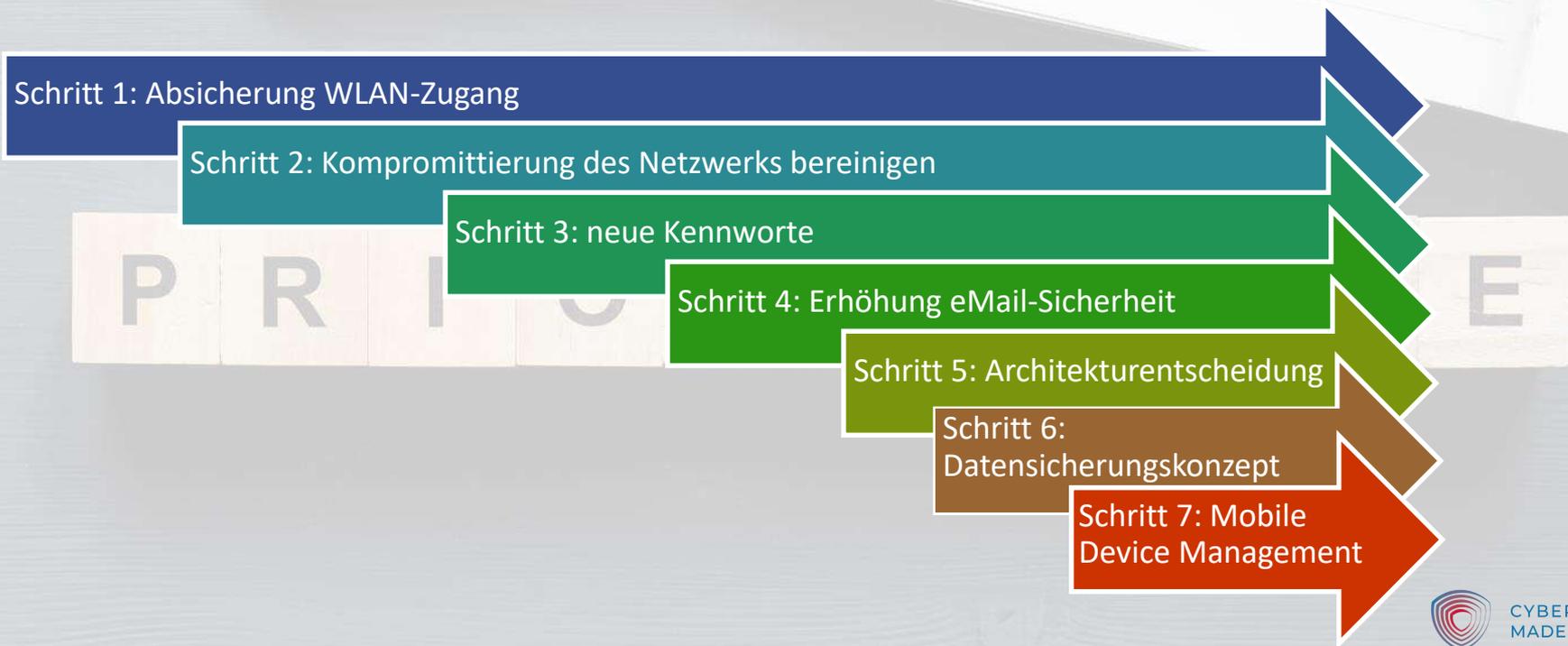
## Ablauf



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

A row of ten light-colored wooden blocks, each with a black letter, spelling out the word 'PRIORITIZEN'. The blocks are arranged horizontally on a dark, textured surface. In the background, a white calendar page is partially visible, showing the time '20:00'.

# 3. bewerten / priorisieren Sie die To Dos



## 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!



## 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](http://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](mailto: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 GeschäftsprozesseDeutscher Excellence Preis 2021 in 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](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>