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

Der unsichtbare Feind:
Wie Cyberkriminelle Ihr Unternehmen bedrohen und wie Sie sich schützen.

Unternehmer*innenfrühstück der Stadt Cham

Tobias Rademann

15. Oktober 2025

Agenda

1. Demo: Cyberangriff
2. Ablauf eines Cyberangriffs
3. effektives Vorgehen zum Schutz Ihres Unternehmens
4. Lessons learned

Kurzprofil: R.iT GmbH

- **Ausrichtung:** iT-Unternehmensberatung
- **Kernthema:** Digitale Transformation Ihres Unternehmens
  - → Managementberatung (Digitale Transformation, Daten/KI)
  - → **iT-Sicherheit**
  - → iT-gestützte Geschäftsprozessoptimierung
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte:** **Region Süd: Cham**
  Zentrale: Bochum
  Region Nord: Bad Schwartau
- **Auszeichnungen:** Ludwig Erhard Preis 2025 in Silber
  TOP100 Innovator 2024 + Top Consultant 2025
  Great Place To Work 2025
  Deutschlands Kunden Champions 2023 Platz 1
  Ecovadis Bronze

Demo: Cyberangriff

gleich in Ihrem Unternehmen…

an dieser Stelle wurde im Vortrag ein Video von einem Angriff mit einem Erpressungstrojaner gezeigt

Das war's!

Ihre Daten sind jetzt *weg.*

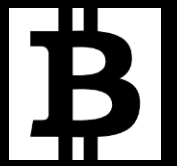
Ihre Daten sind jetzt *weg*.









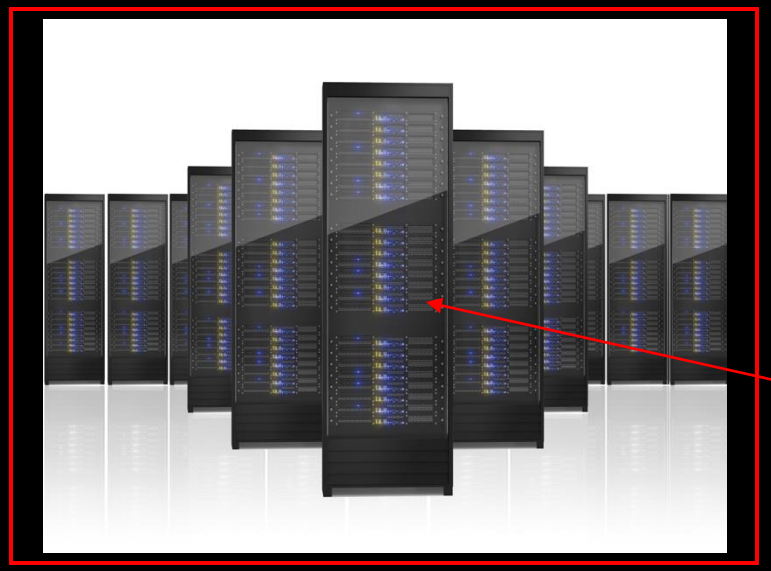



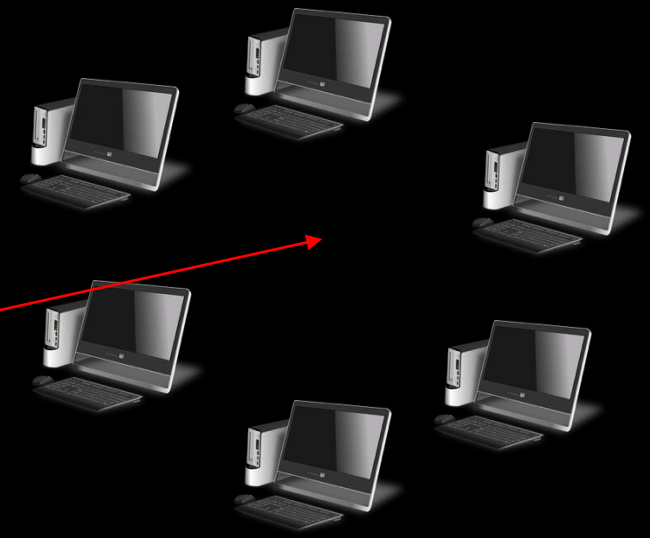

Fall 3: FAI Aviation Group (Nürnberg)

- **Unternehmen:** FAI Aviation Group (FAI rent-a-jet)
  - Standort: Nürnberg (Albrecht-Dürer-Airport) FAI Aviation Group
  - Mitarbeiter: ca. 300 Cybernews FAI Aviation Group (davon 100 Mechaniker/ Ingenieure)
  - Branche: Charterfluggesellschaft, Ambulanzflug, VIP-Flüge, Flugzeugwartung FAI Aviation Group
  - Umsatz: ca. 130-140 Millionen Euro FAI Aviation Group
  - Niederlassungen in Dubai und Bahrain FAI Aviation Group
- **Art des Angriffs:** Ransomware (J Group – neue Gruppe, erstmals Februar 2025 aufgefallen) Security-Insider Cybernews
- **Auswirkungen:**
  - **Datendiebstahl: 2,8 TB an Daten** gestohlen Security-Insider +2
  - Betroffene Daten umfassen:
    - Kundendaten (inkl. Patientendaten aus Ambulanzflugdiensten) Cybernews SC Media
    - Medizinische Informationen von Patienten Cybernews
    - Mitarbeiterdaten, CVs, Passkopien SC Media
    - Geschäftsdokumente und Projektdokumentation Cybernews
    - Audit- und Flugzeugspezifikationsdateien SC Media
    - Mitarbeiter-Trainingsunterlagen SC Media
  - Risiko für Identitätsdiebstahl und Social Engineering Cybernews
  - Erschien auf Dark-Web-Leak-Seite der J Group Security-Insider
- **Datum:** 2025 (vermutlich September/Oktober 2025)

Ihre Systeme stehen *still.*

Ihre Systeme stehen *still.*

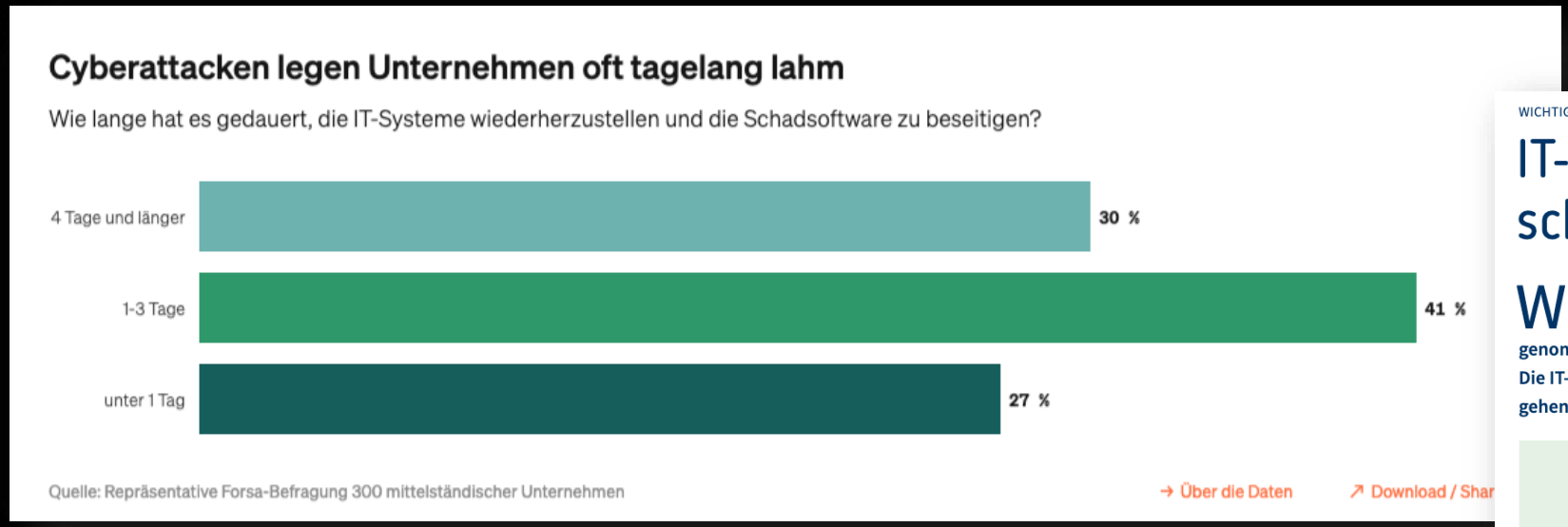




Ihre
Mitarbeiter*innen
sind *verunsichert.*

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

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



Nach dem Cyberangriff auf die IHK-Organisation in Deutschland im August 2022 waren die IT-Systeme je nach Standort unterschiedlich lange betroffen. Die Ausfallzeiten variierten zwischen mehreren Wochen bis zu mehreren Monaten. Einige IHKs konnten bestimmte Dienste erst nach 3-4 Monaten vollständig wiederherstellen. Die komplette Wiederherstellung aller Systeme dauerte bei manchen IHKs bis ins Jahr 2023 hinein.

WICHTIGER HINWEIS

IT-Systeme der IHKs werden schrittweise hochgefahren

Wir bedauern, dass Sie derzeit unsere Webseite nicht in vollem Umfang nutzen können. Aufgrund einer Cyber-Attacke wurden die IT-Systeme der IHKs kontrolliert vom Netz genommen, um möglichen Schaden zu vermeiden und die Datensicherheit zu gewährleisten. Die IT-Systeme werden nach intensiven Prüfungen sukzessive wieder online gestellt. Hierbei gehen Sicherheit und Sorgfalt vor Schnelligkeit.

Die IHKs sind für Sie telefonisch und vor Ort zu erreichen. Die E-Mail-Kommunikation sowie weitere Online-Services (z. B. die Online-Anmeldung zu Veranstaltungen) stehen nicht oder nur eingeschränkt zur Verfügung.

Die Untersuchungen rund um die Cyber-Attacke dauern an. Der technische Dienstleister der Industrie- und Handelskammern, die IHK-GfI, arbeitet dazu mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und Ermittlungsbehörden zusammen. Die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen hat die Ermittlungen übernommen.

Die IHK-Organisation warnt Ihre Mitgliedsunternehmen und Kunden ausdrücklich vor Trittbrettfahrern. **Wenn Zweifel bestehen, ob eine E-Mail wirklich von einer IHK stammt, sollte zur Abklärung eine telefonische Rücksprache erfolgen.**

Bitte entschuldigen Sie die Ihnen hierdurch entstehenden Unannehmlichkeiten.

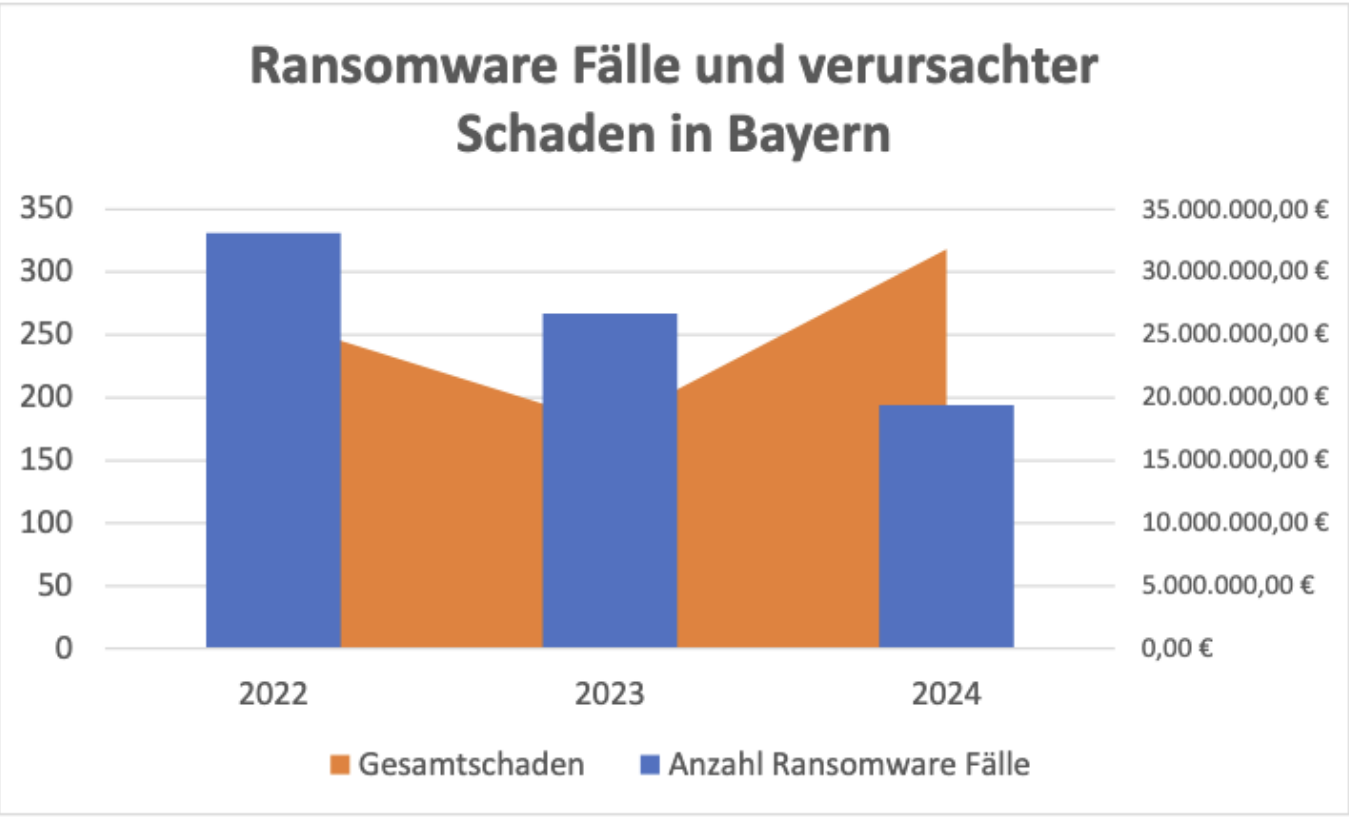
Aktuelle Informationen gibt es unter www.dihk.de

Ihre Kunden bekommen *Angst.*

Und wenden sich *ab*.

Viel Geld steht auf dem Spiel.

Viel Geld steht auf dem Spiel.



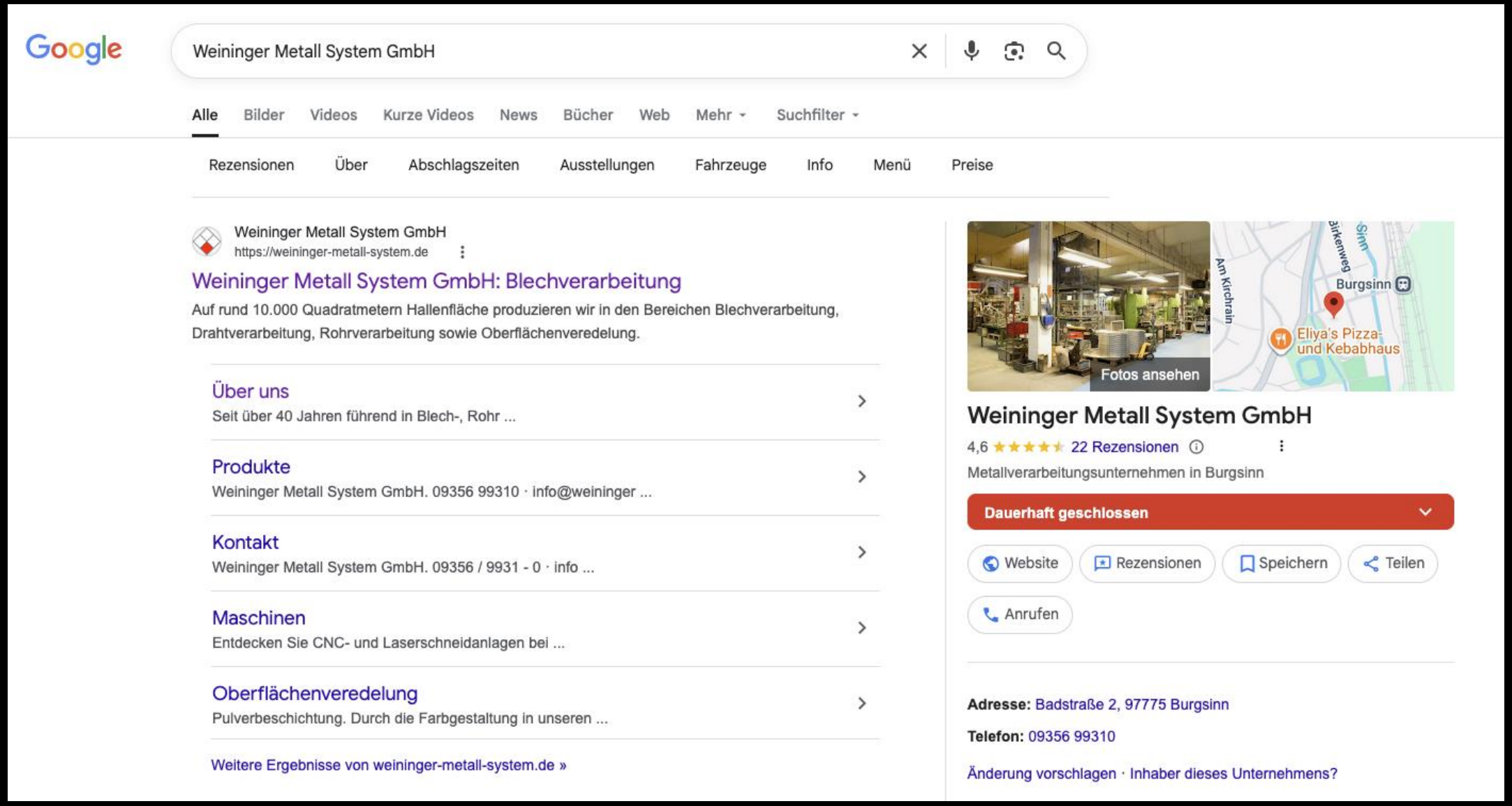
… und die *Existenz*
Ihres Unternehmens!

… und die *Existenz* Ihres Unternehmens!

Fall 2: Weininger Metall System GmbH (Burgsinn bei Würzburg)

- **Unternehmen:** Weininger Metall System GmbH
  - Standort: Burgsinn, Unterfranken (bei Würzburg)
  - Mitarbeiter: 48
  - Branche: Blechbearbeitung, Regalsysteme (Export auch nach China)
  - Familienunternehmen in 2. Generation
- **Art des Angriffs:** Ransomware (8Base-Gruppe)
- **Auswirkungen:**
  - Datendiebstahl: Accounts, Finanzberichte, E-Mails erbeutet
  - Lösegeldforderung mit Veröffentlichungsdrohung
  - **Insolvenzantrag am 21. Februar 2025** beim Amtsgericht Würzburg inFranken
  - Vorläufiger Insolvenzverwalter bestellt inFranken
  - 48 Arbeitsplätze gefährdet inFranken
  - Löhne durch Insolvenzgeld für 3 Monate gesichert inFranken
  - Betrieb sollte zunächst weitergeführt werden
- **Datum:** Januar 2025

… und die *Existenz* Ihres Unternehmens!



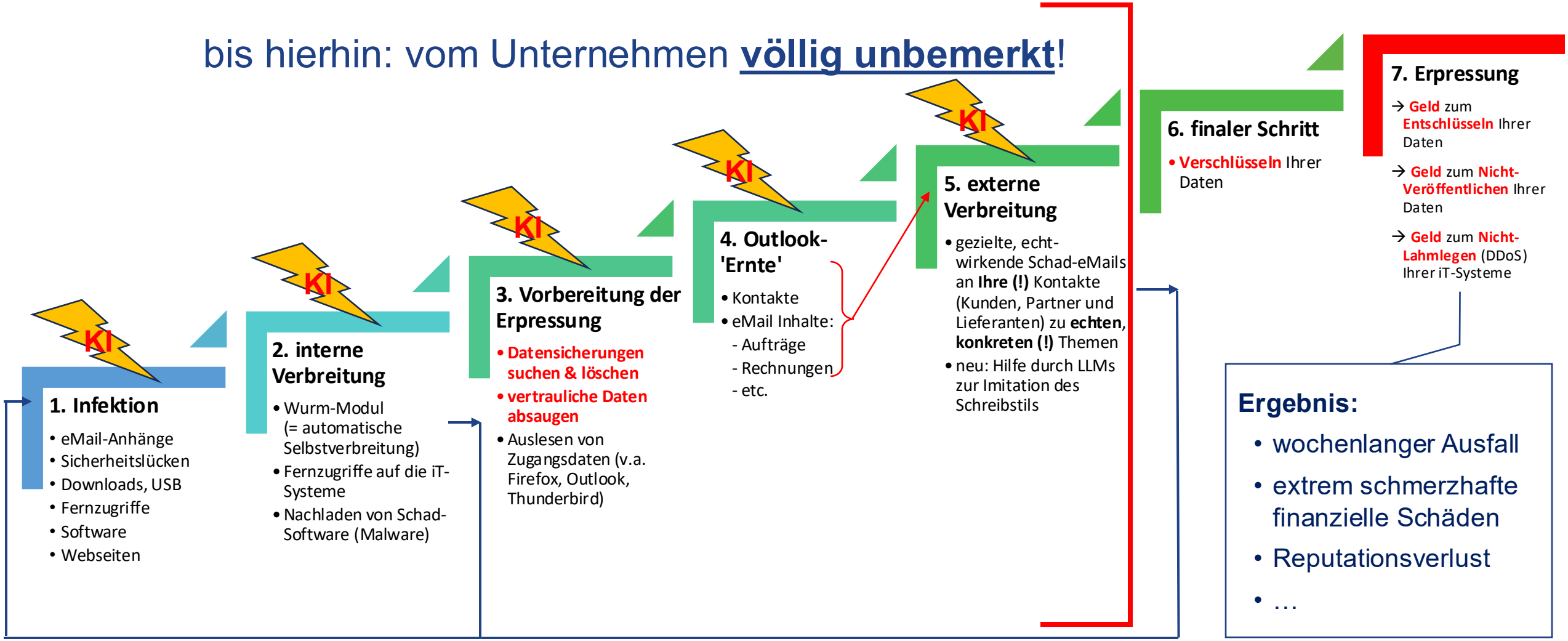
Cyberrisiken sind ***real***.

→ Schützen Sie sich und Ihr Vermächtnis!

2. Ablauf eines Cyberangriffs

Erpressungstrojaner 4.0 ('Tripple Extortion')

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



Ergebnis:

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

3. effektives Vorgehen zum Schutz Ihres Unternehmens

Was tun?

TR Was sind die wichtigsten Sch
Cybersicherheitsrisiken? Bitt

- Multi-Faktor-Authentifizierun
- Regelmäßige Software-Update
- Firewall-Konfiguration
- Endpoint-Schutz (Antivirus/A
- Datensicherung und Backup-S
- Mitarbeiterschulungen zu Phis
- Netzwerksegmentierung
- Privilegierte Zugriffsrechte ver
- Verschlüsselung sensibler Dat
- Incident Response Plan
- Sichere E-Mail-Gateways
- VPN für Remote-Zugriffe
- Regelmäßige Sicherheitsaudit
- Identity and Access Managem
- Mobile Device Management (M
- Sichere Passwort-Richtlinien
- Network Access Control (NAC)
- Security Information and Ever
- Vulnerability Management
- Cyber-Versicherung
- Zero-Trust-Architektur
- Cloud-Sicherheitsmaßnahmer
- Supplier Risk Management
- Business Continuity Planning
- Penetrationstests

TR Sind das die wichtigsten ode rfehlen noch welche?

cybersecurity mittelstand deutschland 2024 2025 — 10 Ergebnisse

Die Liste ist bereits sehr umfassend. Basierend auf den aktuellen Studien und Entwicklungen für 2025 fehlen noch einige wichtige Aspekte:

Zusätzlich wichtige Schutzmaßnahmen:

- Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 Studie Cybersecurity im Mi...
- Chief Information Security Officer (CISO) oder Cyber-Verantwortlicher Studie Cybersecurity im Mi...
- Datenklassifizierung Wirtschaftsschutz: "Unter...
- OT-Sicherheit (Operational Technology) Security-Insider Indevis
- Managed Detection and Response (MDR) Cybersicherheit im Mittels...
- Security Operations Center (SOC) Cybersicherheit im Mittels...
- Malware-Schutz mit aktuellen Signaturen Cybersicherheit Trends 20...
- Notfallplan und Incident Response Team BMWE - Neue CYBERsiche...
- Automated Security Validation / Pentest as a Service Cybersicherheit im Mittels...
- KI-gestützte Bedrohungserkennung Cyberversicherung 2025: B...
- Sichere Homeoffice-Konfiguration BMWE - Cybersicherheit i...
- Supply Chain Security
- NIS-2-Compliance (ab Oktober 2024) Cyberversicherung 2025: B...
- Cyber Threat Intelligence
- Behavioral Analytics
- Secure Coding Guidelines

Die ursprüngliche Liste war bereits sehr gut - diese Ergänzungen machen sie für 2025 vollständig.

Kernfrage

Mit welchen Maßnahmen sollen wir anfangen?

Ihr Action Plan: sinnvolles Vorgehen

Ziel: diejenigen Maßnahmen mit dem **größten Hebel** zuerst angehen

Weg:

1.) Status Quo-**Überblick** schaffen

2.) Maßnahmen **priorisieren**

in Abstimmung auf Ihr Budget:

3.) **schrittweise & regelmäßig** nächst-priorisierte Maßnahme umsetzen

+

mit einem kompetenten Partner

1. Verschaffen Sie sich einen Überblick

1. 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 (= 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**.

Fall 2

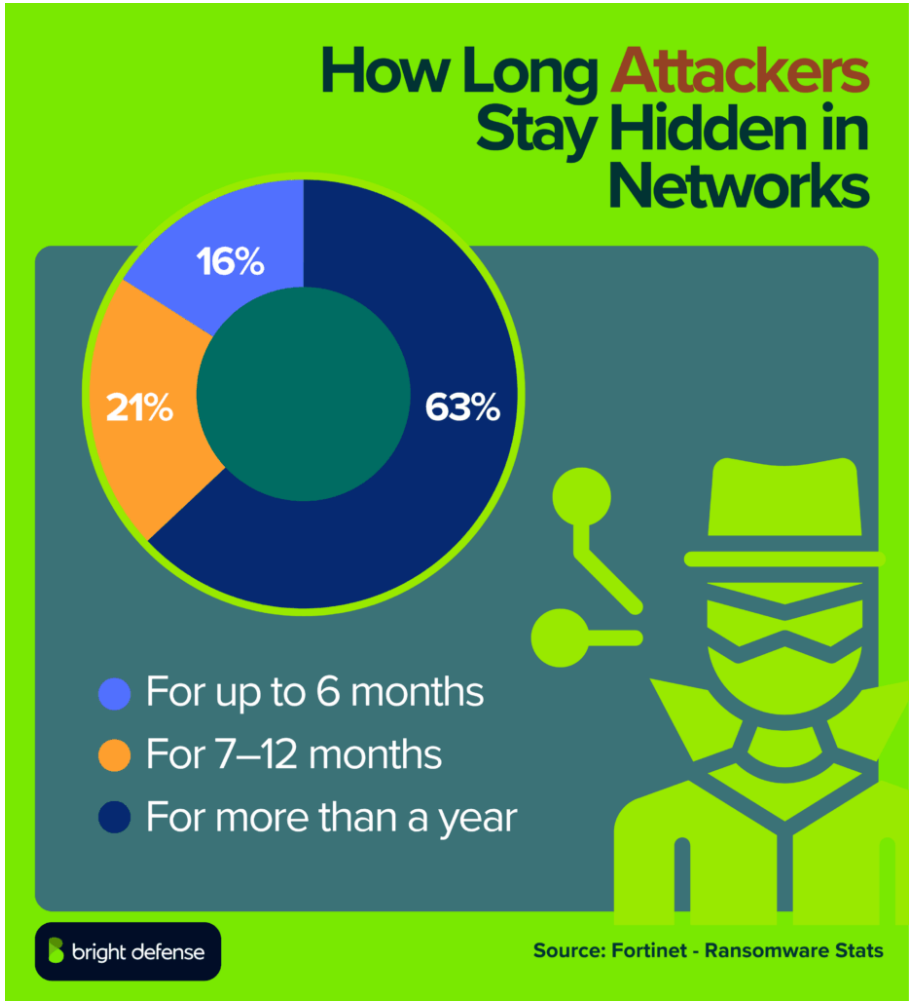
Angebotsbesprechung 'iT Risk Assessment'

- 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**

Fall 2



1. Verschaffen Sie sich einen Überblick

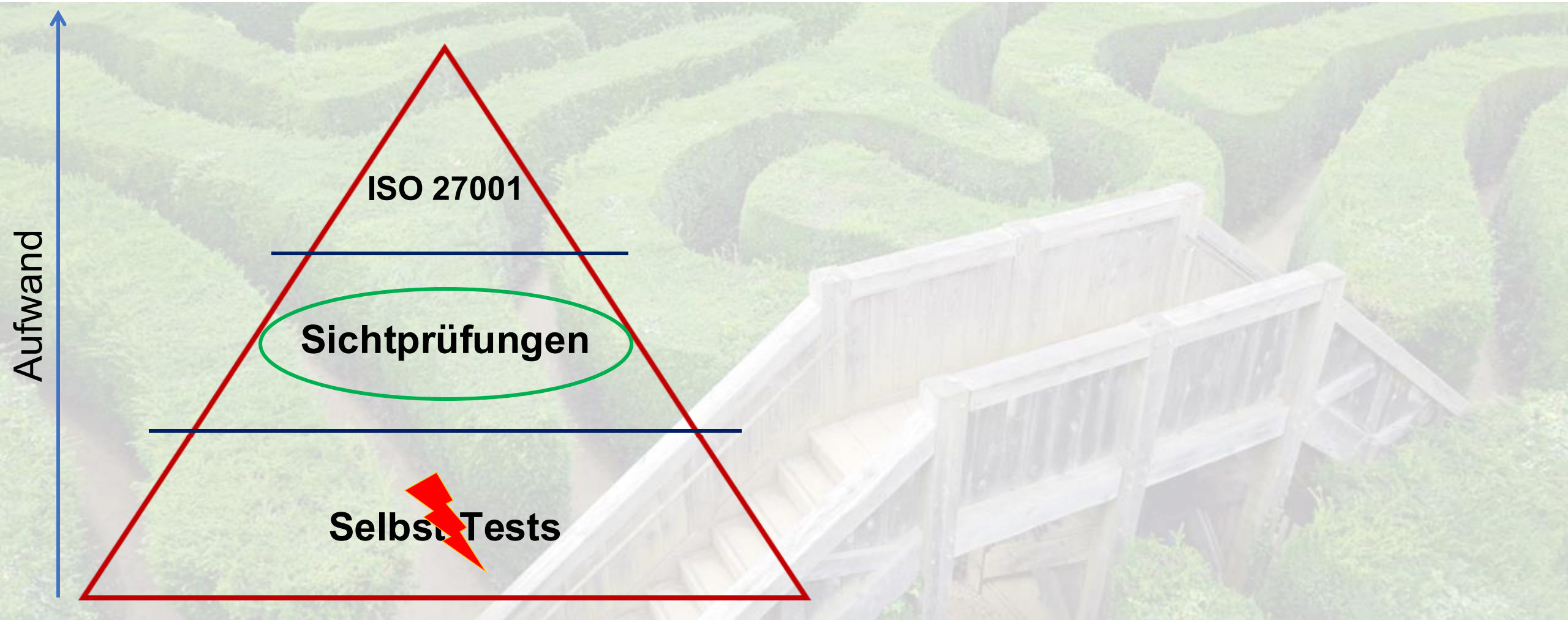
Warum keine Selbst-Tests?

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

Gründe für Fehler:

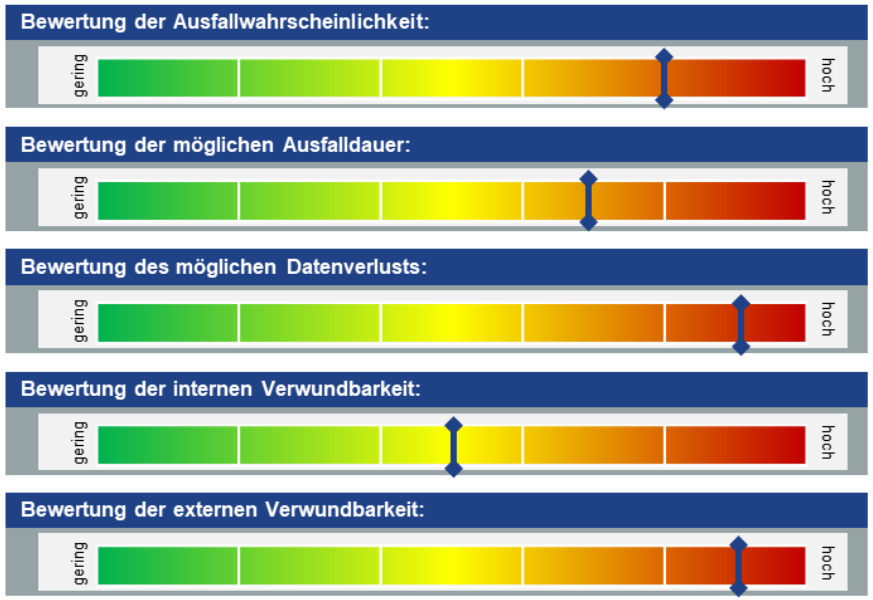
- fehlendes Wissen
- fehlende Erfahrung
- Flüchtigkeitsfehler

1. Verschaffen Sie sich einen Überblick



Vorteile Sichtprüfung

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

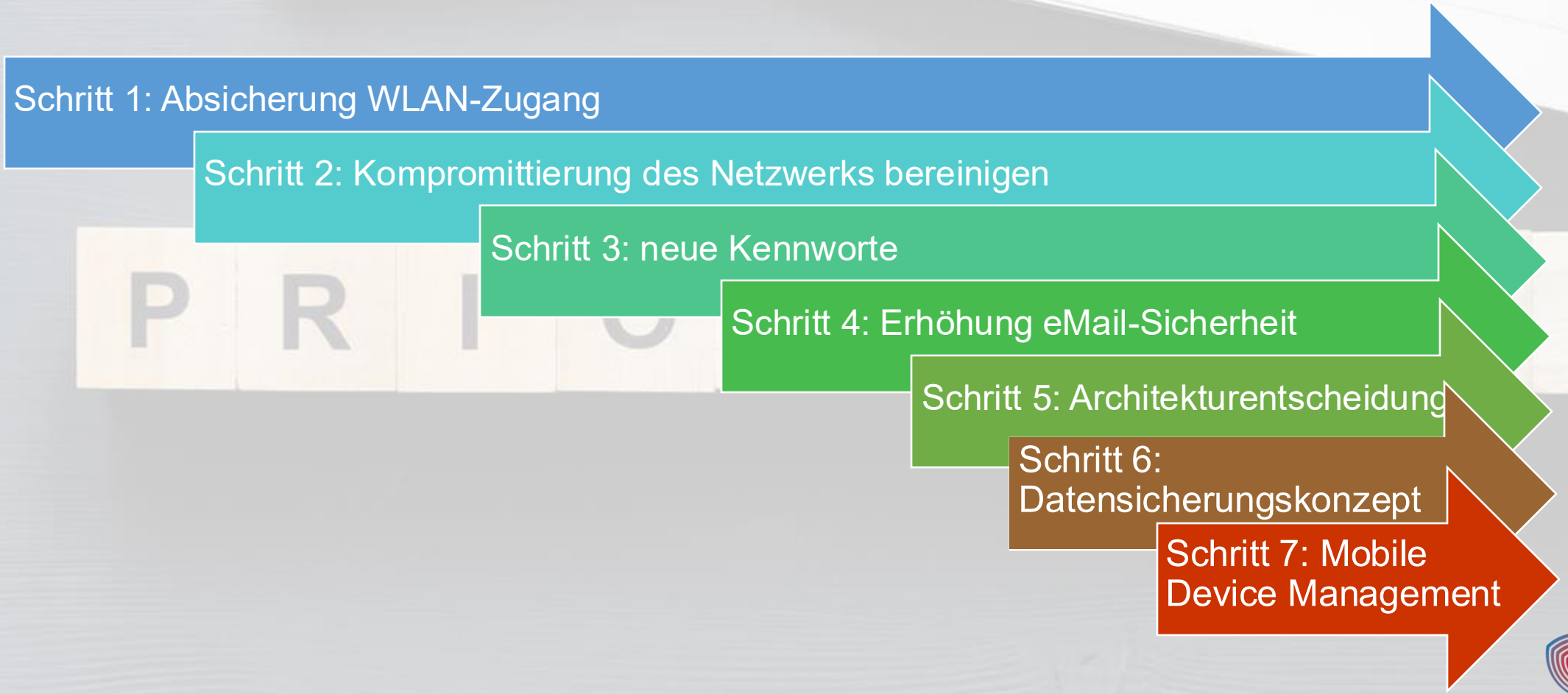


CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

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

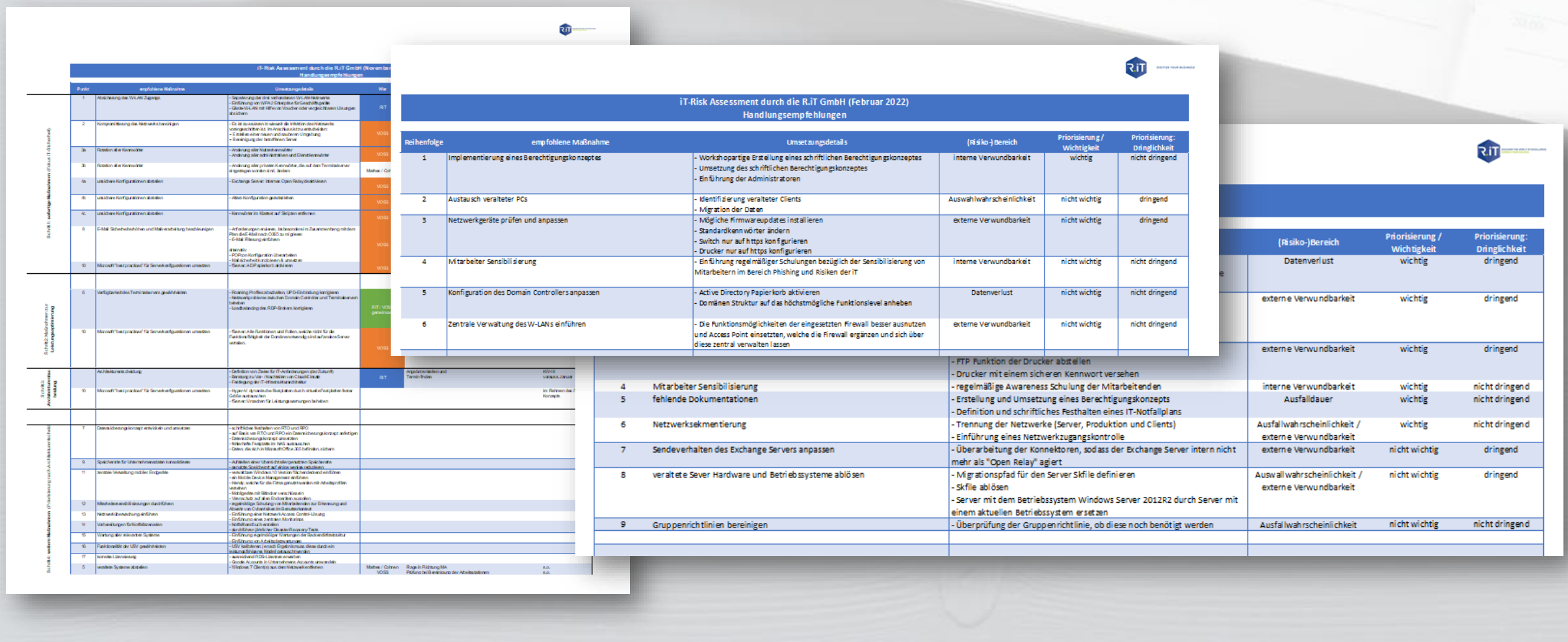
2. bewerten / priorisieren Sie die To Dos



CYBERSECURITY MADE IN EUROPE™

Initiated by ECSO. Issued by eurobits e.V.

3. priorisieren Sie die To Dos



iT-Risk Assessment durch die R.iT GmbH (Februar 2022)
Handlungsempfehlungen

Reihenfolge	empfohlene Maßnahme	Umsetzungsdetails	(Risiko-)Bereich	Priorisierung / Wichtigkeit	Priorisierung: Dringlichkeit
1	Implementierung eines Berechtigungskonzeptes	- Workshopartige Erstellung eines schriftlichen Berechtigungskonzeptes - Umsetzung des schriftlichen Berechtigungskonzeptes - Einführung der Administratoren	interne Verwundbarkeit	wichtig	nicht dringend
2	Austausch veralteter PCs	- Identifizierung veralteter Clients - Migration der Daten	Auswahlwahrscheinlichkeit	nicht wichtig	dringend
3	Netzwerkgeräte prüfen und anpassen	- Mögliche Firmwareupdates installieren - Standardkennwörter ändern - Switch nur auf https konfigurieren - Drucker nur auf https konfigurieren	externe Verwundbarkeit	nicht wichtig	dringend
4	Mitarbeiter Sensibilisierung	- Einführung regelmäßiger Schulungen bezüglich der Sensibilisierung von Mitarbeitern im Bereich Phishing und Risiken der IT	interne Verwundbarkeit	nicht wichtig	nicht dringend
5	Konfiguration des Domain Controllers anpassen	- Active Directory Papierkorb aktivieren - Domänen Struktur auf das höchstmögliche Funktionslevel anheben	Datenverlust	nicht wichtig	nicht dringend
6	Zentrale Verwaltung des W-LANs einführen	- Die Funktionsmöglichkeiten der eingesetzten Firewall besser ausnutzen und Access Point einsetzten, welche die Firewall ergänzen und sich über diese zentral verwalten lassen	externe Verwundbarkeit	nicht wichtig	nicht dringend

			(Risiko-)Bereich	Priorisierung / Wichtigkeit	Priorisierung: Dringlichkeit
			Datenverlust	wichtig	dringend
			externe Verwundbarkeit	wichtig	dringend
			externe Verwundbarkeit	wichtig	dringend
		- FTP Funktion der Drucker abstellen - Drucker mit einem sicheren Kennwort versehen			
4	Mitarbeiter Sensibilisierung	- regelmäßige Awareness Schulung der Mitarbeitenden	interne Verwundbarkeit	wichtig	nicht dringend
5	fehlende Dokumentationen	- Erstellung und Umsetzung eines Berechtigungskonzepts - Definition und schriftliches Festhalten eines IT-Notfallplans	Ausfalldauer	wichtig	nicht dringend
6	Netzwerksekmentierung	- Trennung der Netzwerke (Server, Produktion und Clients) - Einführung eines Netzwerkzugangskontrolle	Ausfallwahrscheinlichkeit / externe Verwundbarkeit	wichtig	nicht dringend
7	Sendeverhalten des Exchange Servers anpassen	- Überarbeitung der Konnektoren, sodass der Exchange Server intern nicht mehr als "Open Relay" agiert	externe Verwundbarkeit	nicht wichtig	dringend
8	veraltete Sever Hardware und Betriebssysteme ablösen	- Migrationspfad für den Server 5kfile definieren - 5kfile ablösen - Server mit dem Betriebssystem Windows Server 2012R2 durch Server mit einem aktuellen Betriebssystem ersetzen	Auswallwahrscheinlichkeit / externe Verwundbarkeit	nicht wichtig	dringend
9	Gruppenrichtlinien bereinigen	- Überprüfung der Gruppenrichtlinie, ob diese noch benötigt werden	Ausfallwahrscheinlichkeit	nicht wichtig	nicht dringend

3. beginnen Sie mit der Umsetzung

3. beginnen Sie mit der Umsetzung

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

effektive Schutzmaßnahmen: **must-haves**

TÄGLICHE DATENSICHERUNG (GETESTET)

OFFLINE (!) DATENSICHERUNG

SICHERHEITS-UPDATES

MULTI-FAKTOR AUTHENTIFIZIERUNG

MITARBEITER*INNEN-SENSIBILISIERUNG

effektive Schutzmaßnahmen: nice-to-haves

PASSWORT-MANAGER

ANTI-SPAM GATEWAY

MOBILE DEVICE MANAGEMENT

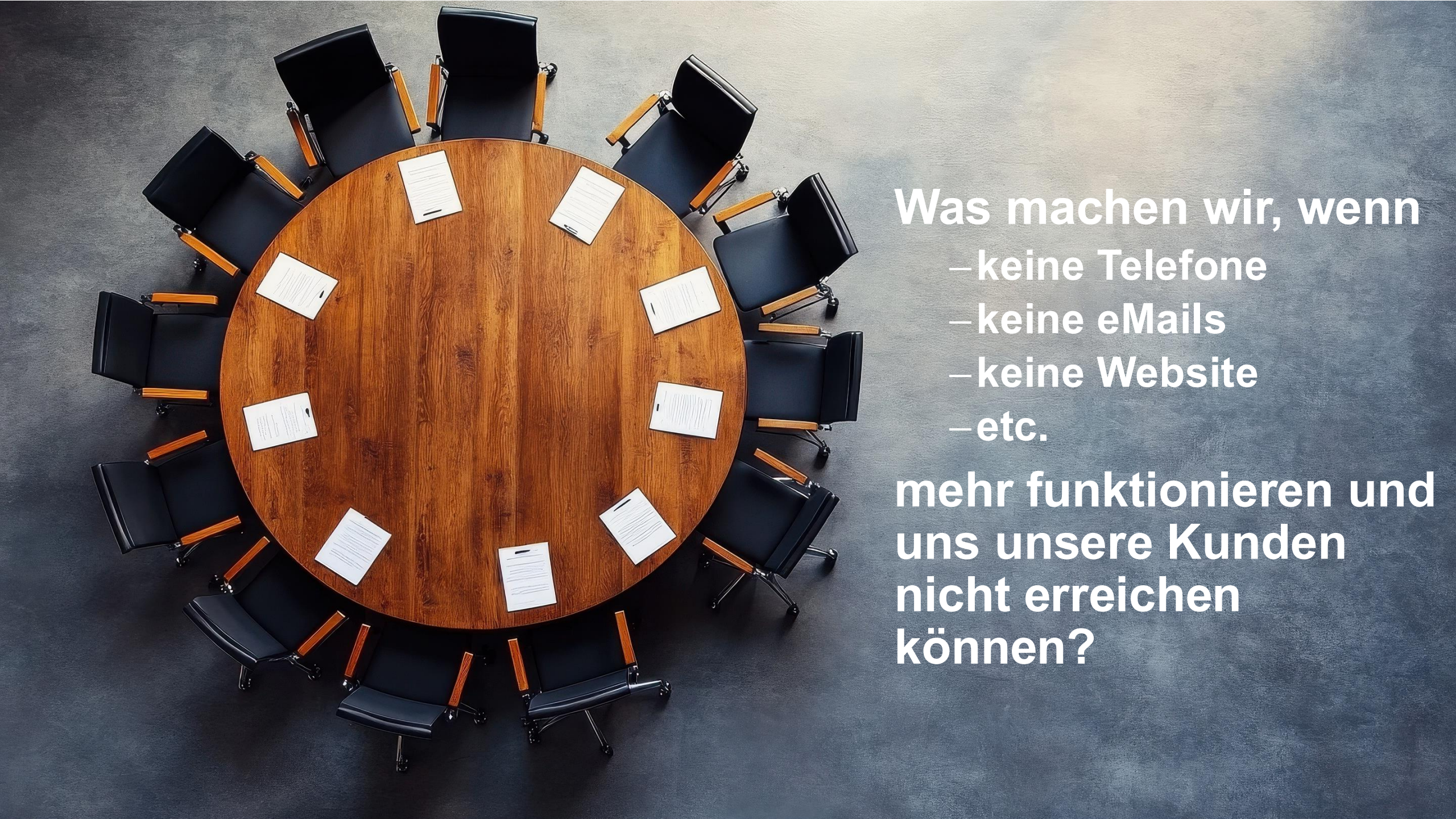
ZUGRIFFS-BEDINGUNGEN

MONITORING / KI-BASIERTE ANALYSE

ZENTRALER ENDGERÄTESCHUTZ

VERSCHLÜSSELUNG (DATEN, KANÄLE)


Wie überweisen
wir Bitcoins?



Was machen wir, wenn

- keine Telefone
- keine eMails
- keine Website
- etc.

mehr funktionieren und uns unsere Kunden nicht erreichen können?

effektiver Schutz = angemessene (Re-)aktion

effektiver Schutz Ihres Unternehmens

- ***vor*** einem Cyberangriff
- ***während*** eines Cyberangriffs
- ***nach*** einem Cyberangriff

➔ effektiver Schutz Ihres Unternehmens umfasst **auch und gerade** die Phase, in der Sie erfolgreich angegriffen wurden

4. Résumée

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.

Konsequenzen: Handeln Sie – ***jetzt***!

1. **sorgen Sie für eine Grundlage**
   - regelmäßige Sensibilisierung von Anwender*innen
   - regelmäßige Sicherheitsupdates
   - physisch getrennte, regelmäßige und getestete (!) Backups
   - Kommunikationsstrategie
2. **arbeiten Sie systematisch: Überblick, Priorisierung, nächster Schritt**
3. **machen Sie iT-Sicherheit zur Gewohnheit**
   - proaktiv
   - zielgerichtet
   - regelmäßig

→ mit kleinen, aber kontinuierlichen Schritten viel erreichen

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

NL Süd: Rodinger Str. 15, 93413 Cham
Tel.: (09971) 806 29-0, Fax: -29

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