BVMW
Bundesverband
mittelständische Wirtschaft

R.iT

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

Hacker lieben den Mittelstand:
Cyberangriffe, Datendiebstahl, Deepfakes – und Ihr Unternehmen mittendrin.

BVMW Internet & Digitalisierung

Tobias Rademann

15. April 2025

Agenda

1. Warum Zuhören lohnt – auch um diese Uhrzeit ;-)
2. Mittestand im Fokus
3. Bedrohungsszenarien
4. effektiver Schutz vor Cyberrisiken
5. Résumée: lessons learned

Kurzprofil: R.iT GmbH

- **Ausrichtung:** iT-Unternehmensberatung
- **Kernthema:** Digitale Transformation Ihres Unternehmens
  → Managementberatung (Dig. 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
  Great Place To Work 2023
  Deutschlands Kunden Champions 2023 Platz 1

1. Warum Zuhören lohnt – auch um diese Uhrzeit ;-)


morgen früh in Ihrem Unternehmen…

an dieser Stelle wurde ein Video zu einem Hacking-Angriff auf ein Unternehmen gezeigt

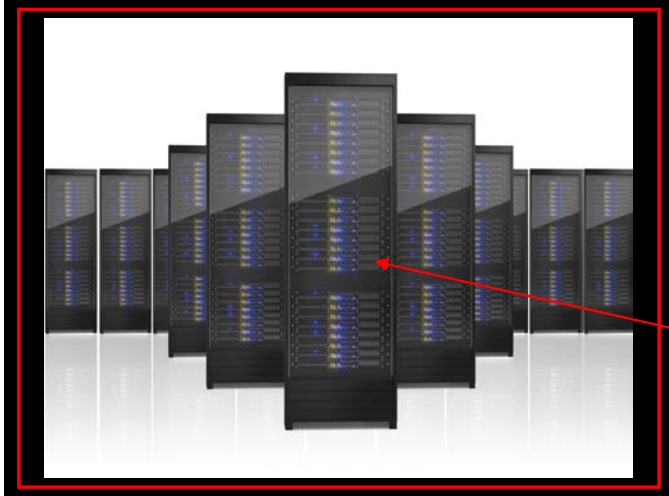
Das war's!

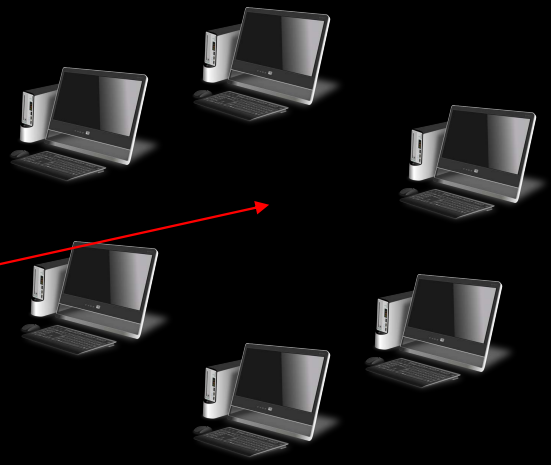
Ihre Daten sind jetzt *weg.*

Ihre Daten sind jetzt *weg*.

Ihre Systeme stehen *still.*

Ihre Systeme stehen *still*.

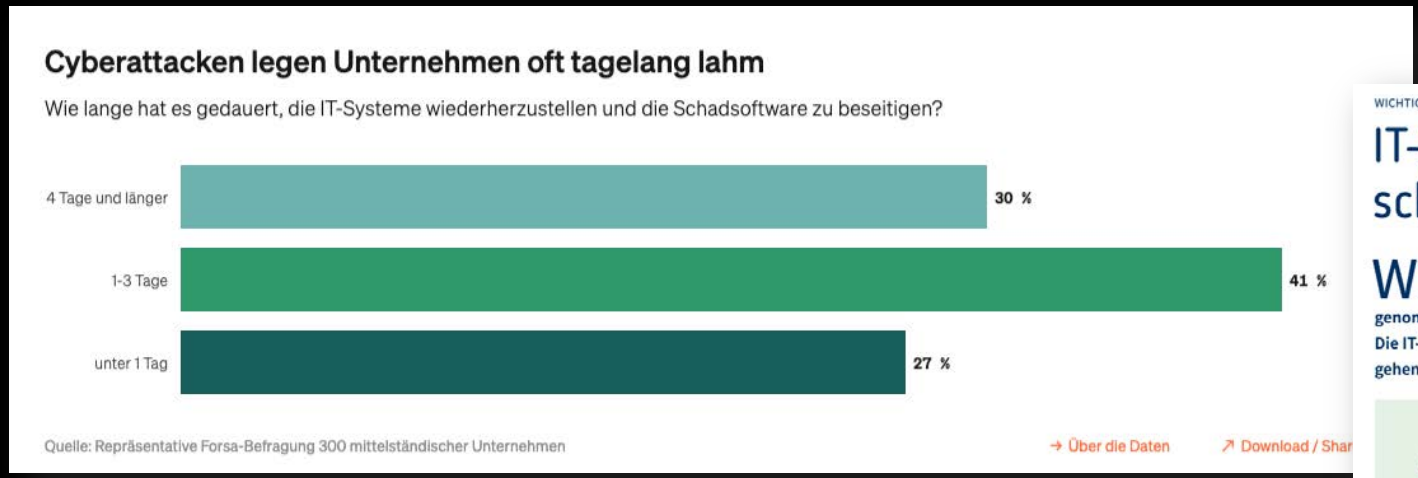




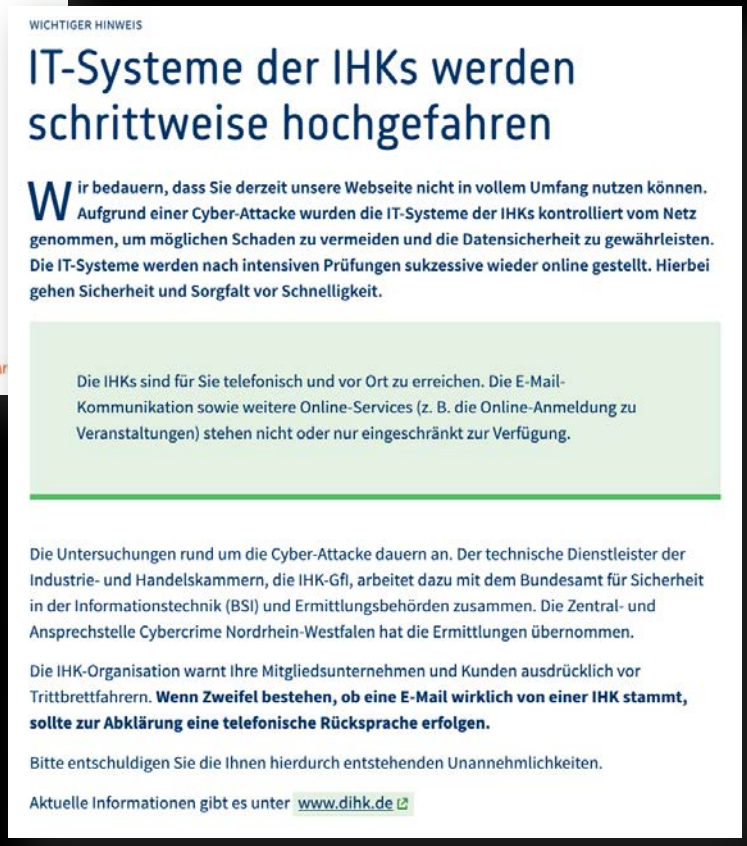
Ihre
Mitarbeiter*innen
sind *verunsichert.*

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.



Ihre Kunden
bekommen *Angst.*

Und wenden sich *ab*.

Viel Geld steht auf dem Spiel.

… und die *Existenz*
Ihres Unternehmens!

… und die *Existenz* Ihres Unternehmens!

Startseite › Wirtschaft

Verschlimmerte Lage durch Cyberattacke: Traditionsunternehmen mit über 400 Beschäftigten ist insolvent

17.10.2024, 18:03 Uhr
Von: Bona Hyun

Unternehmen aus Aachen ist insolvent – Cyberattacke führte zu Produktionsausfällen

Die Schumag AG habe einen Antrag auf Sanierung in Eigenverwaltung beim zuständigen Amtsgericht Aache n gestellt, heißt es in einer Pressemitteilung des Unternehmens vom 9. Oktober. Die aktuell rund 450 Beschäftigten des Unternehmens wurden vom Vorstand und dem Team der Eigenverwaltung bereits über die aktuellen Entwicklungen und die nächsten Schritte informiert. Der operative Geschäftsbetrieb wird weiter fortgeführt; Löhne und Gehälter seien über das Insolvenzgeld gesichert.

Prophete: Insolvenz nach Cyber-Angriff

Insolvenz des Fahrradherstellers belegt Bedeutung von IT-Sicherheit

Insolvenz nach mehrwöchigem Systemausfall

Fahrradhersteller nach Cyber-Angriff vollständig lahmgelegt

Gefahr für Geschäftsgeheimnisse und personenbezogene Daten

Hohes Haftungsrisiko für Geschäftsführer

NEWS > BUSINESS

Nach Cyberangriff und Corona-Pandemie: Maschinenbauer stellt Insolvenzantrag

09.02.2025 08:00 | Von: Jessica von Thun

Cyberrisiken sind ***real***.

→ Schützen Sie sich und Ihr Vermächtnis!

2. Mittelstand im Fokus

Mittelstand im Fokus

- Konzerne haben gehandelt ✓

Mittelstand im Fokus

- Konzerne ~~haben gehandelt~~ ***mussten*** handeln
  - ✓Schutzniveau deutlich erhöht
  - ✓Prozesse vorhanden
  - ✓Ansprechpartner vorhanden

KRITIS

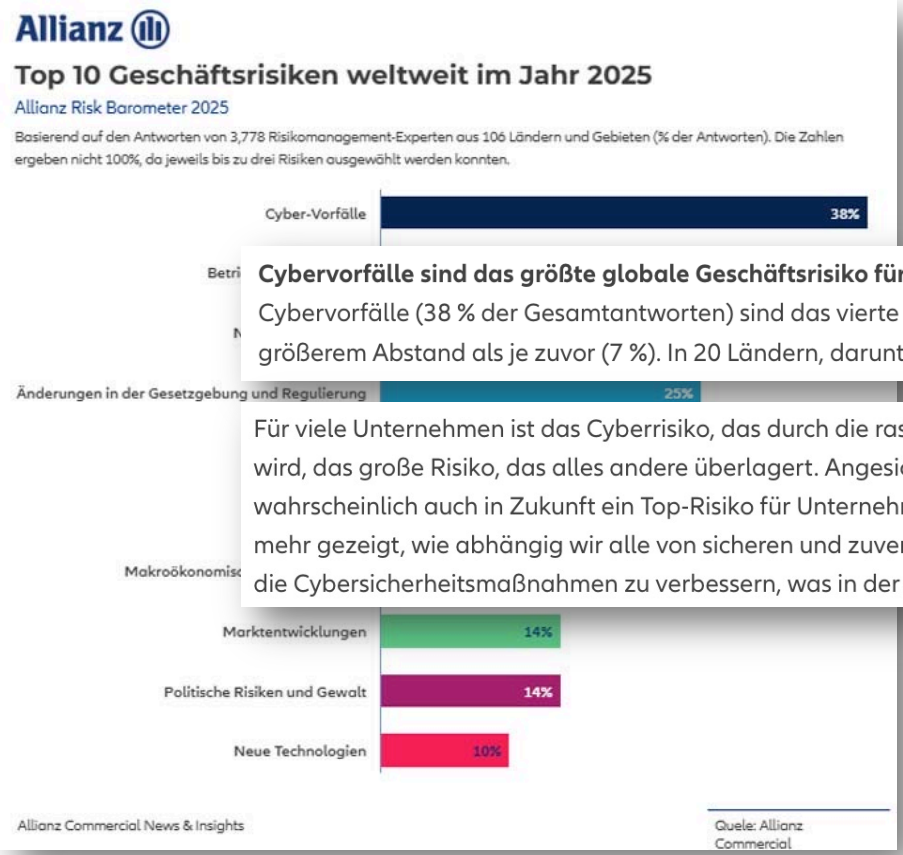
- Mittelstand: größere Unternehmen ***müssen jetzt*** handeln

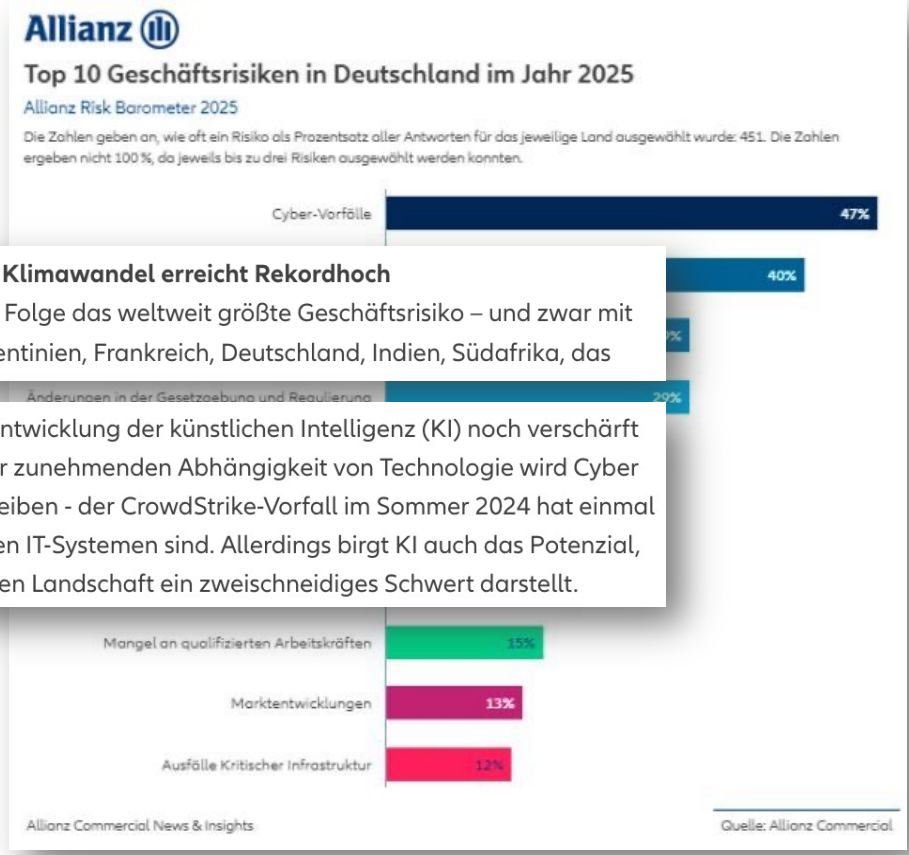
NIS-2 Richtlinie

- Der Rest: kann warten

  …und wird damit ***unvergleichlich attraktiv*** für Hacker!

Top 10 Geschäftsrisiken (Allianz AG)





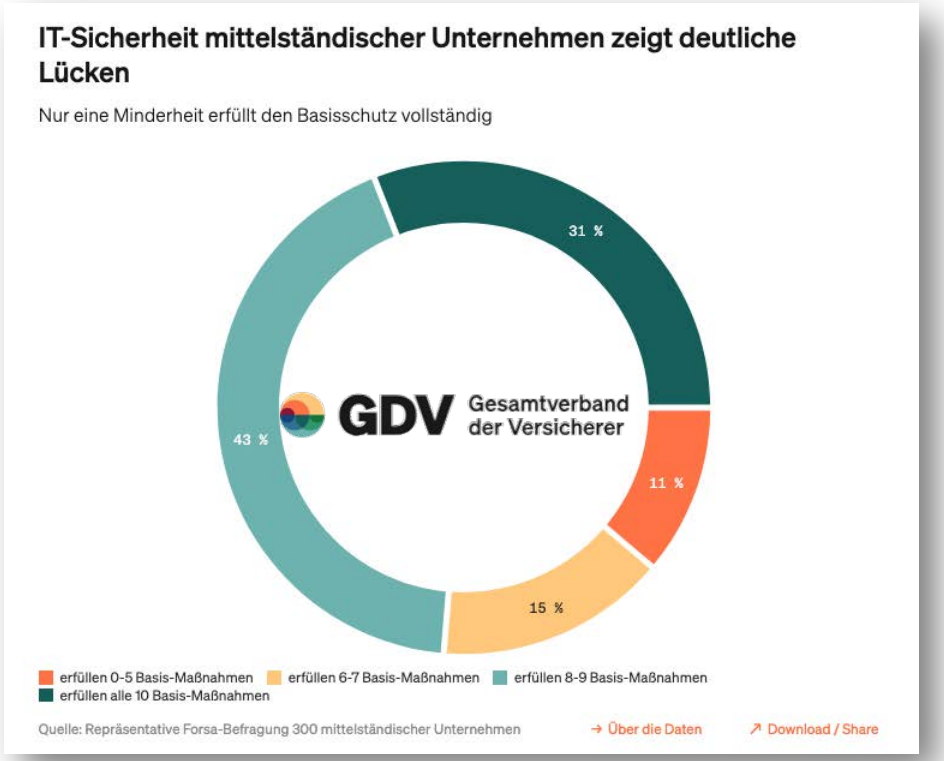
Cybervorfälle sind das größte globale Geschäftsrisiko für 2025; Klimawandel erreicht Rekordhoch

Cybervorfälle (38 % der Gesamtantworten) sind das vierte Jahr in Folge das weltweit größte Geschäftsrisiko – und zwar mit größerem Abstand als je zuvor (7 %). In 20 Ländern, darunter Argentinien, Frankreich, Deutschland, Indien, Südafrika, das

Für viele Unternehmen ist das Cyberrisiko, das durch die rasante Entwicklung der künstlichen Intelligenz (KI) noch verschärft wird, das große Risiko, das alles andere überlagert. Angesichts der zunehmenden Abhängigkeit von Technologie wird Cyber wahrscheinlich auch in Zukunft ein Top-Risiko für Unternehmen bleiben - der CrowdStrike-Vorfall im Sommer 2024 hat einmal mehr gezeigt, wie abhängig wir alle von sicheren und zuverlässigen IT-Systemen sind. Allerdings birgt KI auch das Potenzial, die Cybersicherheitsmaßnahmen zu verbessern, was in der digitalen Landschaft ein zweischneidiges Schwert darstellt.

Status Quo im Mittelstand

Zwei Drittel der mittelständischen Unternehmen haben Sicherheitslücken



IT-Sicherheit mittelständischer Unternehmen zeigt deutliche Lücken

Die Grafik zeigt, in welchem Umfang mittelständische Unternehmen den Basisschutz erfüllen. Die zehn Basis-Schutzmaßnahmen entsprechen grundliegenden Obliegenheiten der GDV-Musterbedingungen für eine Cyberversicherung. Hier geht es unter anderem um Passwörter und Zugänge, Schutz vor Schadsoftware, Datensicherungen und Sicherheitsupdates. Die konkreten Basis-Schutzmaßnahmen finden Sie unter www.gdv.de/cybercheck.

Diese Grafik stammt aus einer repräsentativen Forsa-Umfrage im Auftrag des GDV. Im Rahmen seiner Initiative CyberSicher beauftragt der GDV die Forsa Gesellschaft für Sozialforschung und statistische Analysen mbH seit 2018 jährlich mit einer repräsentativen Befragung von 300 Entscheidern und IT-Verantwortlichen von kleinen und mittleren Unternehmen zu ihrer Wahrnehmung von Cyberrisken und den IT-Sicherheitsmaßnahmen der Unternehmen.

Zuletzt aktualisiert: **19.12.2024**

Cybersicherheit

Versicherer sehen kaum Fortschritte bei der IT-Sicherheit deutscher Unternehmen

Mit einer Mischung aus Überschätzung der eigenen IT-Sicherheit und Verharmlosung der Gefahr reagiert der Mittelstand auf die Cyberbedrohung. Die Folge: Wichtige Sicherheitsvorkehrungen unterbleiben, wie eine Umfrage im Auftrag des GDV zeigt.

Zuletzt aktualisiert: **19.12.2024** • Lesedauer **19min.**

Quelle: https://www.gdv.de/gdv/medien/medieninformationen/it-sicherheit-mittelstaendischer-unternehmen-zeigt-deutliche-luecken-185036

Zwischenfazit

KMUs sind das **attraktivste Ziel** für Hacker!

3. Bedrohungsszenarien


KI + Cyberrisiken = Deepfakes

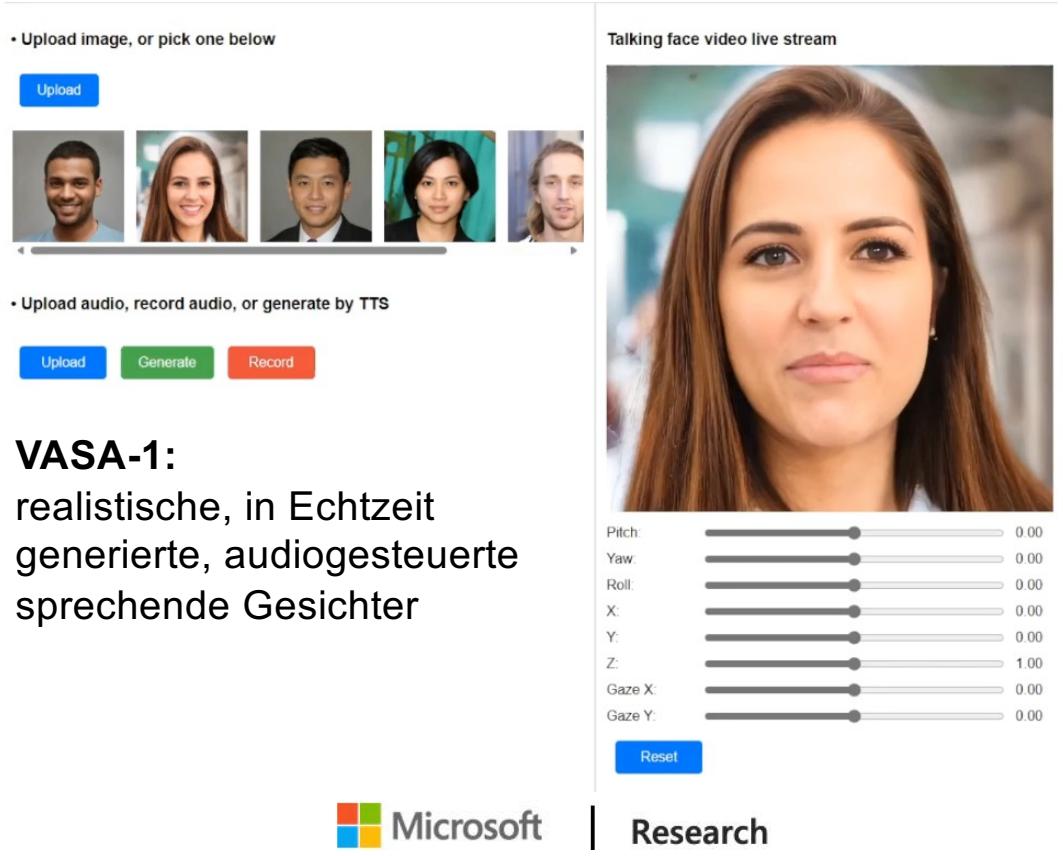
Deepfakes

Deep + **Fake**

→ **Ziel:** Erschaffung **künstlicher** (von GenAI generierter) Medieninhalte,

Deepfakes: Beispiele

1. **Text**
   - Text-Generierung
2. **Stimme**
   - Text-zu-Sprache
   - Stimmenkonvertierung
3. **Fotos: Gesichter**
   - Face Swapping
4. **Videos**
   - Face Reenactment



VASA-1:
realistische, in Echtzeit generierte, audiogesteuerte sprechende Gesichter

Deepfakes: Beispiele

1. **Text**
   - Text-Generierung
2. **Stimme**
   - Text-zu-Sprache
   - Stimmenkonvertierung
3. **Gesichter**
   - Face Swapping
4. **Videos**
   - Face Reenactment
   - künstliche Situationen


Cyberrisiken + Künstliche Intelligenz
= neue Dimension der Bedrohung

Die neue Dimension der Cyberrisiken

- Phishing Mails v2
- Erpressungstrojaner v4
- Rufschädigung v2
- Erpressung v2
- CEO-Fraud v2

Phishing / Social Engineering v2

Phishing / Social Engineering

Wichtig: Bitte aktualisieren Sie Ihre Daten von ING. - Posteingang - tra@rit.de

Löschen | Archivieren | Melden | Verschieben | Kennzeichnung löschen | Als gelesen markieren | Synchronisieren

Zusammenfassung durch Copilot — Zusammenfassen

Extern **Wichtig: Bitte aktualisieren Sie Ihre Daten von ING.**

E — ING-DiBa <evdzm27682@synergy-group.com.my>

Sonntag, 6. April 2025 um 23:27

Erledigt am Donnerstag, 10. April 2025.

Zur Onlineversion

ING

Wichtige Information: Aktualisieren Sie Ihre ING-App.

Sehr geehrter Kunde,

Um weiterhin alle Funktionen und höchsten Sicherheitsstandards Ihrer ING-App zu gewährleisten, bitten wir Sie, diese auf die neueste Version zu aktualisieren.

Folgen Sie bitte dem untenstehenden Link, um die Aktualisierung durchzuführen:

App Aktualisieren

https://pay.mizbanwp.com/~cp54507/xss

Vielen Dank für Ihre Aufmerksamkeit.

Mit freundlichen Grüßen,

Ihr ING-Team

Sicherheit | Abmelden | YouTube

Holen Sie sich die App **für iOS** — Laden im App Store

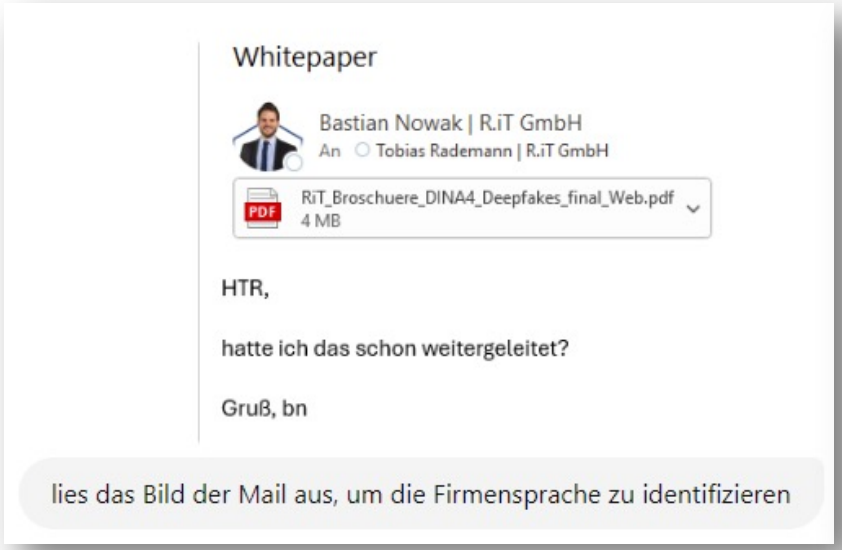
Holen Sie sich die App **für Android** — JETZT BEI Google Play

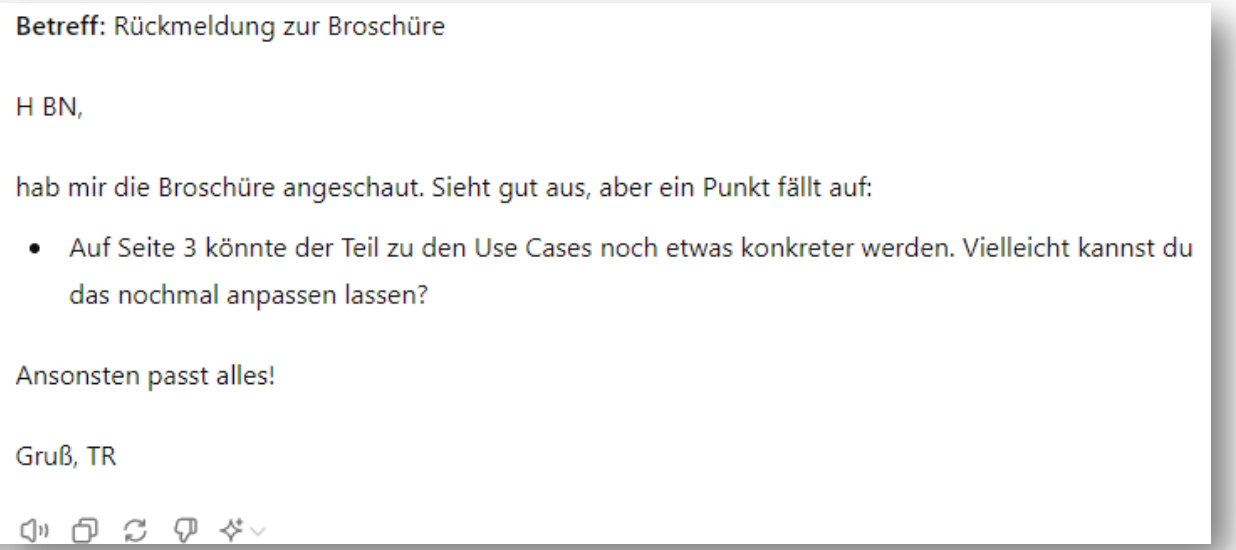
ING-DiBa AG
Theodor-Heuss-Allee 2
60486 Frankfurt am Main

Phishing / Social Engineering v2

- **Ziel:** Erlangung sensibler Informationen (→ Emotionen, Neugierde)
- **mögliche Anwendungsfälle**
  - vertrauenswürdige Informationen / Zugänge preisgeben
  - Schadsoftware herunterladen
- **neu**
  - !: imitierte Formulierungen vertrauenswürdiger Personen
    → Nutzung von LLMs!
- **Auswirkungen**
  - vglsw. hoch, da **potentiell alle Mitarbeiter*innen mögliche Ziele**
  - Phishing / Social Engineering i.d.R. **'nur' Vorstufe / Einstieg**

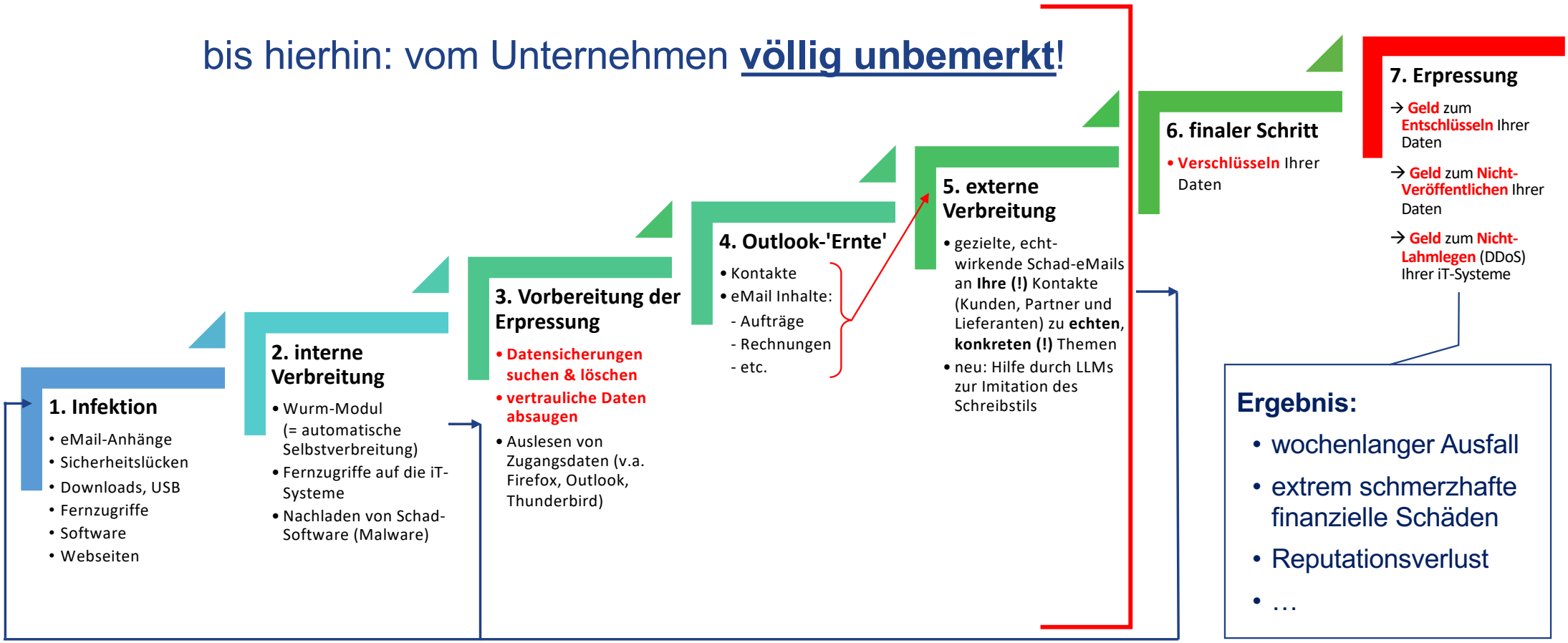
Phishing / Social Engineering v2






Erpressungstrojaner v4

Erpressungstrojaner 4.0 ('Tripple Extortion')




Rufschädigung

Rufschädigung

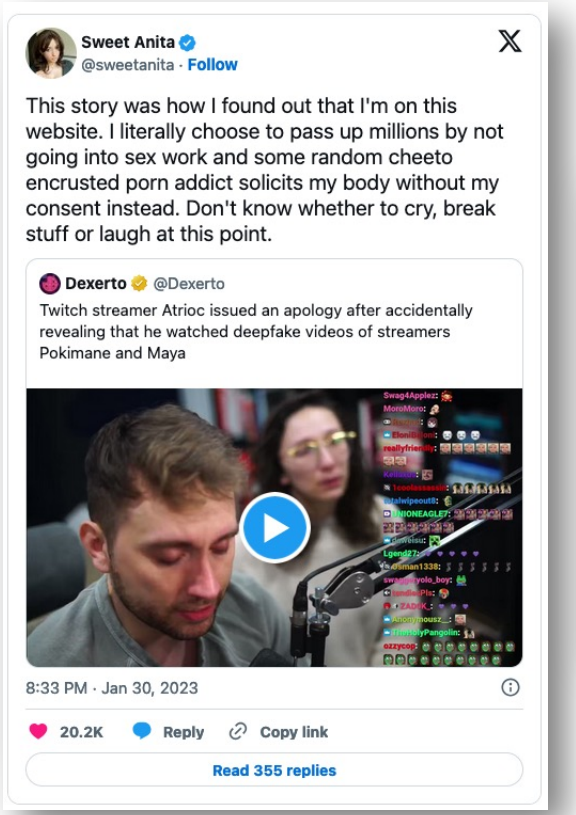
- **Ziel:** Schädigung **des Ansehens / der Glaubwürdigkeit** einer bestimmten Person, Organisation oder Gruppe
- **mögliche Anwendungsfälle**
  - Falschaussagen, Anschwärzungen
  - kompromittierende & kontroverse Situation
  - Ereignis, das nicht existiert oder anders abgelaufen ist
  - falsche Beweise in (Gerichts-)Verfahren
  - die schlichte Behauptung, vorgelegte Beweise seien Deepfakes
- **neu**: falsche Medieninhalte (Deepfakes)
- **Auswirkungen**
  - bei Vorbereitung: eher gering bis mittel
  - ohne Vorbereitung: vglsw. hoch

Rufschädigung – Beispiele

Rufschädigung – Beispiele

Deepfake-Pornografie von Twitch-Streamerinnen (2023)

Rufschädigung – Beispiele

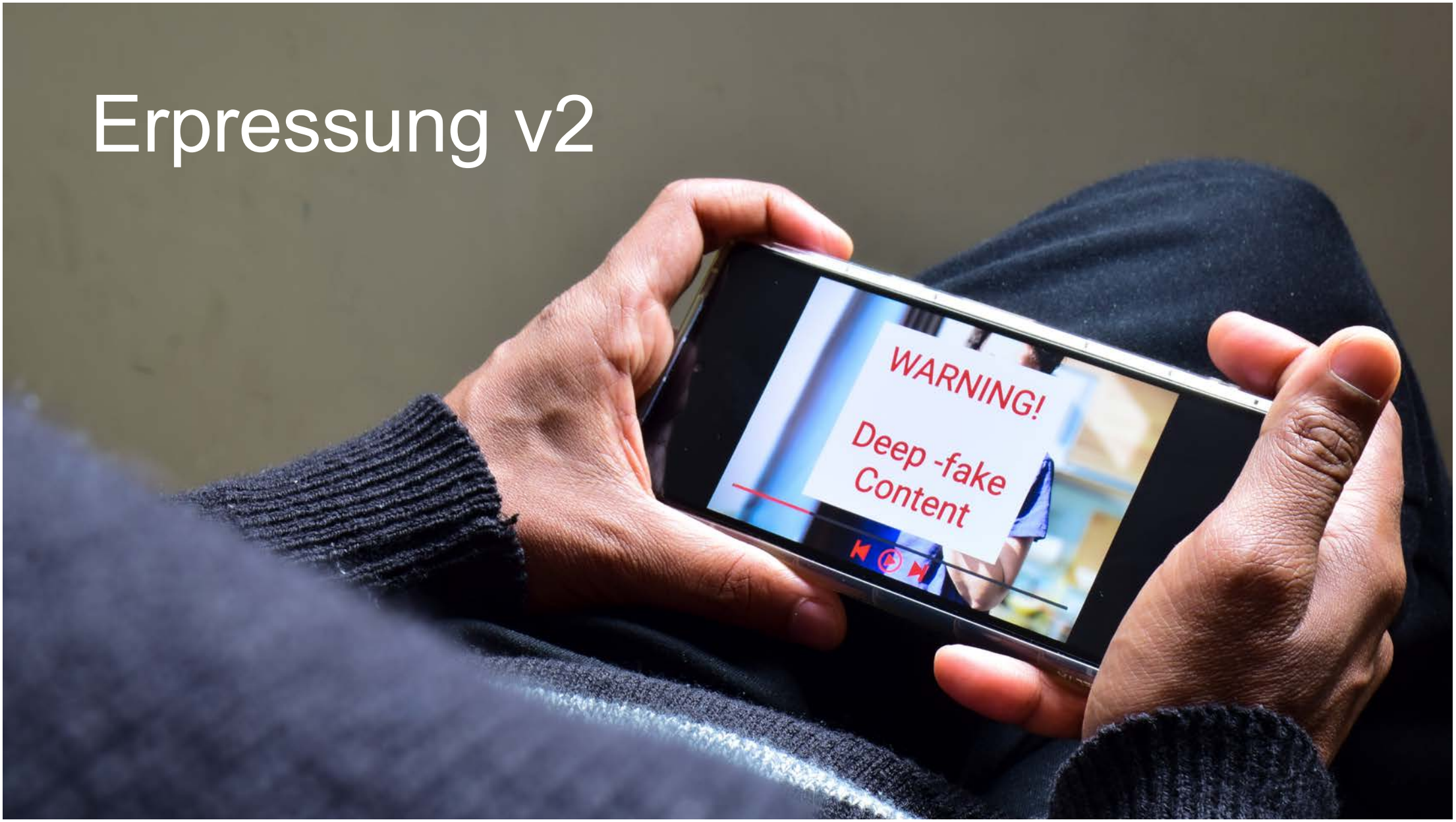


Deepfake-Pornografie von Twitch-Streamerinnen (2023)

Rufschädigung – Beispiele

Deepfake-Pornografie von Twitch-Streamerinnen (2023)

Erpressung v2



Erpressung

- **Ziel:** Erpressung von **Geld** oder **sensiblen Informationen / Zugängen** einzelner Individuen (seltener: Unternehmen)
- **mögliche Anwendungsfälle + Beispiele**
  - *s.o., 'Rufschädigung'*
- **Auswirkungen**
  - extrem hoch, → **alle Mitarbeiter*innen mögliche Erpressungsziele**
  - Erpressungsangriffe i.d.R. 'nur' Vorstufe / Einstieg
  - kaum bis keine technische Schutzmaßnahmen mgl.
  - → FBI (06/23): explizite Warnung vor einem signifikanten Anstieg von Erpressungsfällen durch Deepfake-basierte Bilder und Videos

CEO-Fraud v2

CEO-Fraud / Chef-Betrug (alte Version)

bisher: ***eMails***

Aufbau von ***Druck***

Einbezug ***unbekannter Autoritätspersonen***

CEO-Fraud / Chef-Betrug v2

- **Ziel:** Überweisung hoher Geldbeträge
- **neu:** Deepfakes von **Stimmen und Videos bekannter (!), entsprechend befugter Entscheider*innen**
- **Beispiele**
  - ARUP: Überweisung von US$ 24 Mio. in 12 Transaktionen (01/2024)
  - Ferrari: CEO Anruf zu geheimer Übernahme (fehlgeschlagen) (07/2024)
  - Überweisungen bei deutschen Banken
- **Auswirkungen**
  - kurz- bis mittelfristige Liquiditätsprobleme
  - Imageschaden


3. effektive Schutzmaßnahmen

effektive Schutzmaßnahmen: **must-haves**

TÄGLICHE DATENSICHERUNG

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)

effektive Schutzmaßnahmen: Ergebnis

➔ **Risikominimierung** ist möglich ✓

… aber:

- ✓ kostet Geld
- ✓ kostet Zeit
- ✓ ist umfangreich und vielschichtig

→ v.a. **Antwort auf eine Kernfrage** wichtig:

Mit welcher Maßnahme 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.
  - Eine offsite-Datensicherung war **nicht vorhanden**.
  - Das Kennwort für den Zugriff auf die Datensicherung lag **im Klartext** vor.

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**

1. Verschaffen Sie sich einen Überblick

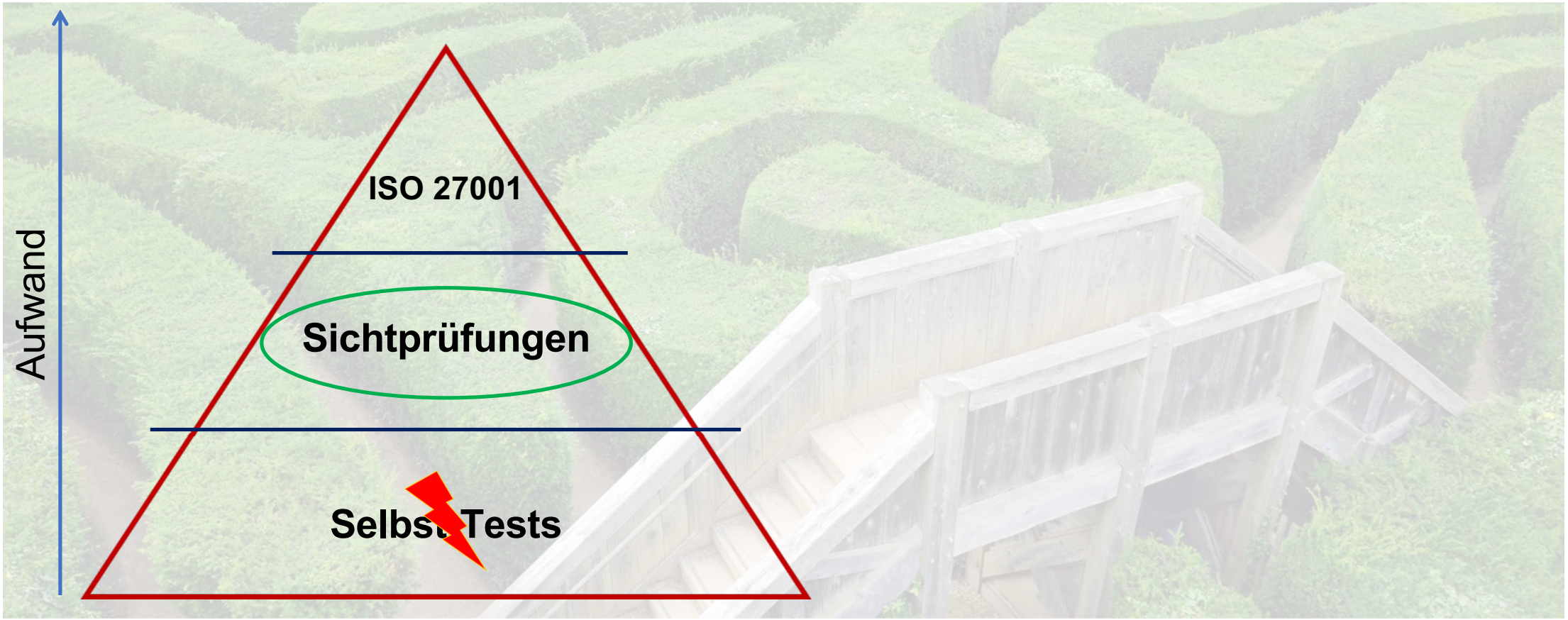
Warum keine Selbst-Tests?

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

Gründe für Fehler:

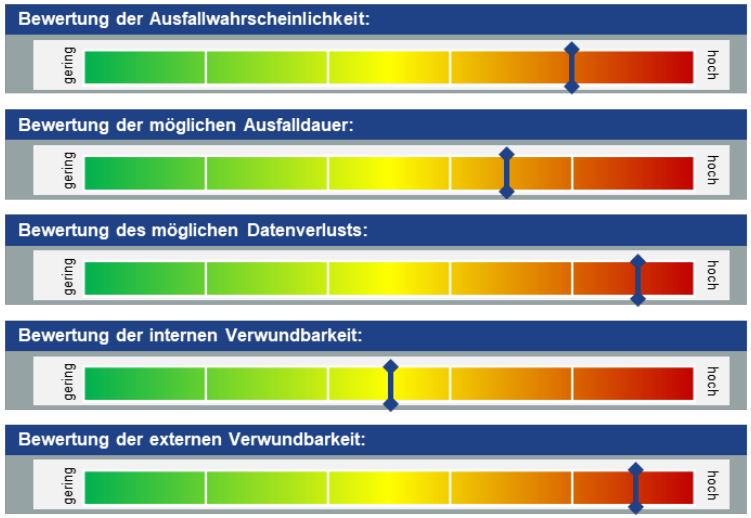
- fehlendes Wissen
- fehlende Erfahrung
- Flüchtigkeitsfehler

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

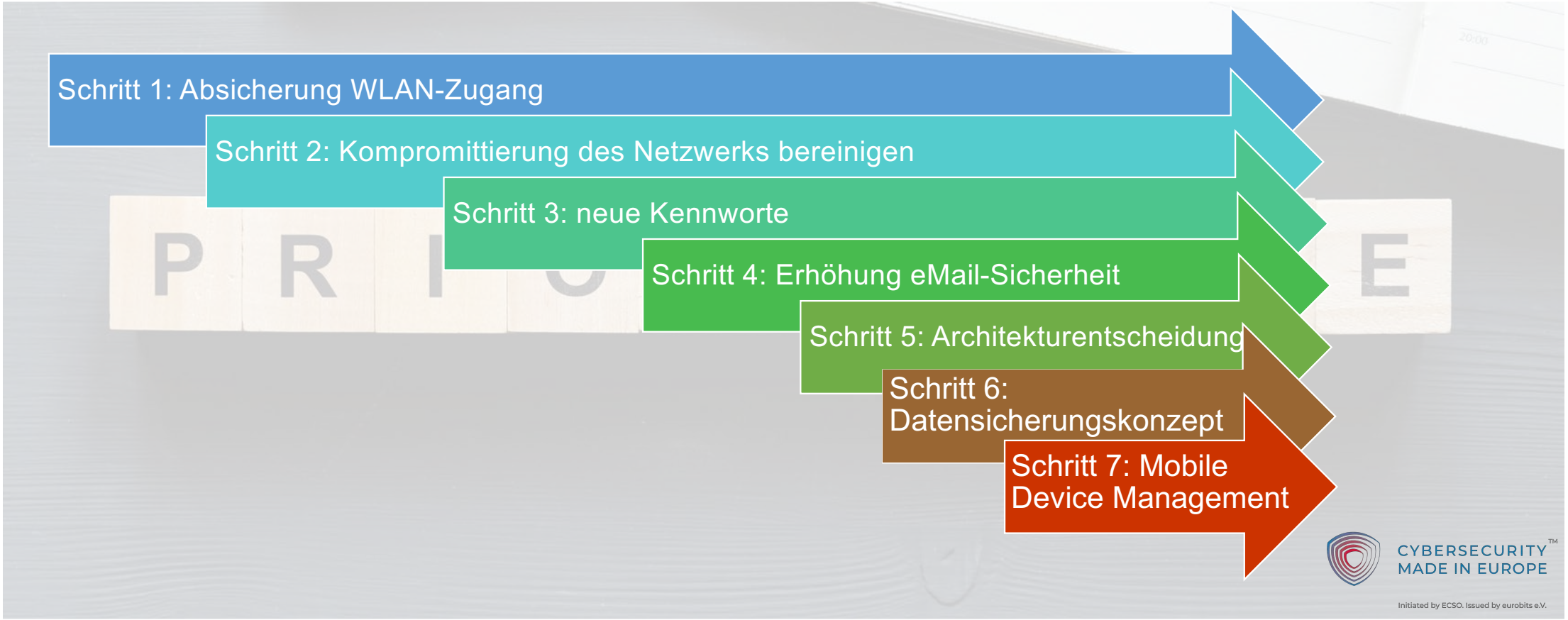


CYBERSECURITY™
MADE IN EUROPE

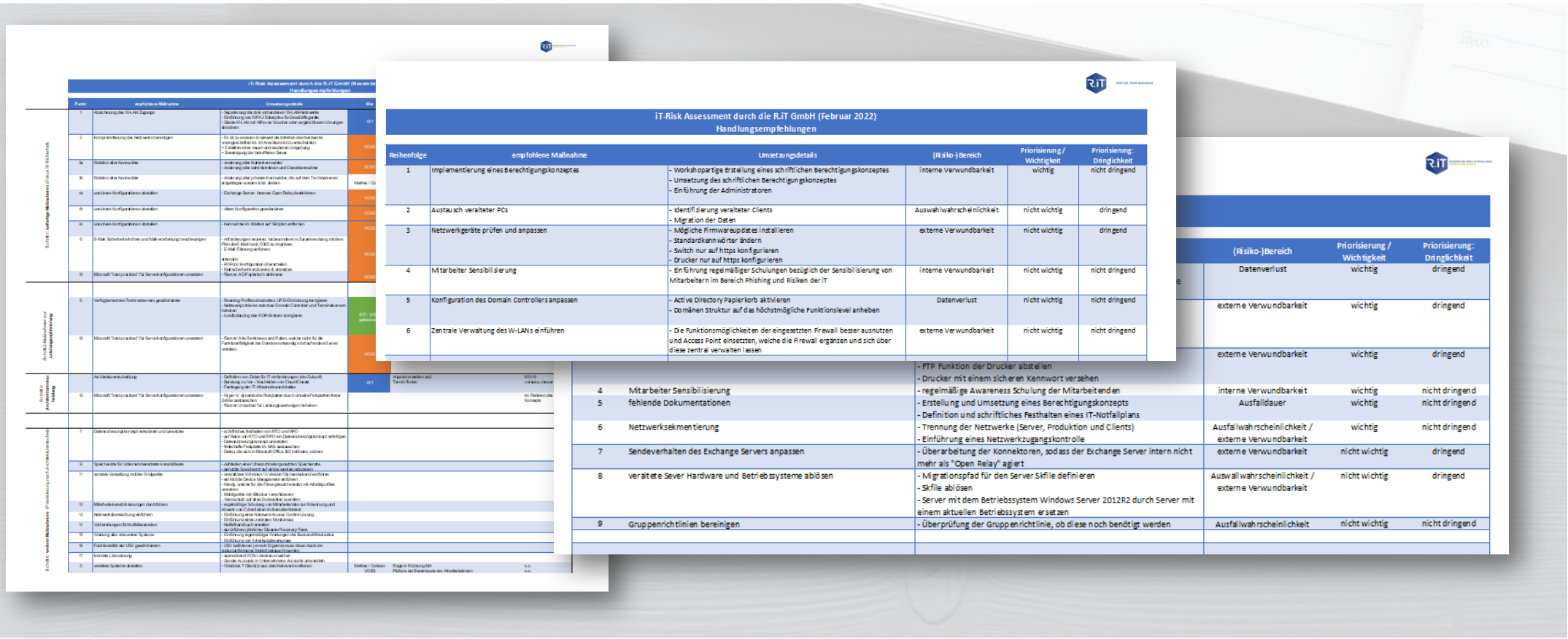
Initiated by ECSO. Issued by eurobits e.V.

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

2. bewerten / priorisieren Sie die To Dos



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

		- FTP Funktion der Drucker abstellen - Drucker mit einem sicheren Kennwort versehen	externe Verwundbarkeit	wichtig	dringend
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 Skfile definieren - Skfile ablösen - Server mit dem Betriebssystem Windows Server 2012R2 durch Server mit einem aktuellen Betriebssystem ersetzen	Auswahlwahrscheinlichkeit / 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

5. Résumée

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

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

Unternehmensgröße, Kontostand, Branche sind egal.

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

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

1. **sorgen Sie für eine Grundlage**
   - regelmäßige Sicherheitsupdates
   - physisch getrennte, regelmäßige Backups
   - regelmäßige Sensibilisierung von Anwendern
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