



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. Mittelstand im Fokus
3. Bedrohungsszenarien
4. effektiver Schutz vor Cyberrisiken
5. Résumé: lessons learned



Kurzprofil: R.iT GmbH



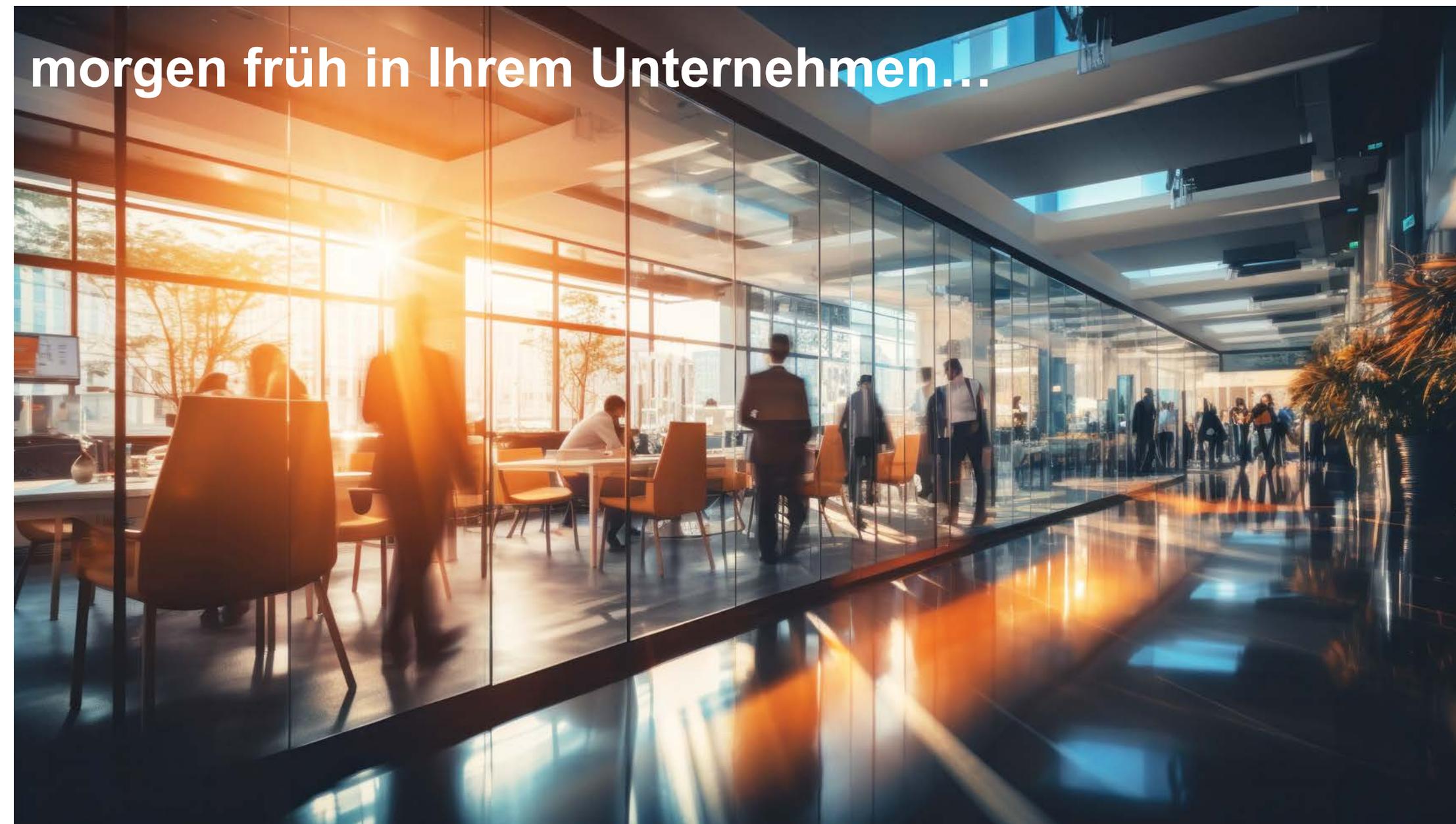
- **Ausrichtung:** iT-Unternehmensberatung
- **Kernthema:** Digitale Transformation Ihres Unternehmens
 - Managementberatung (Dig. Transformation, Daten/KI)
 - **iT-Sicherheit**
 - iT-gestützte Geschäftsprozessoptimierung
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte:**
 - Region 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!

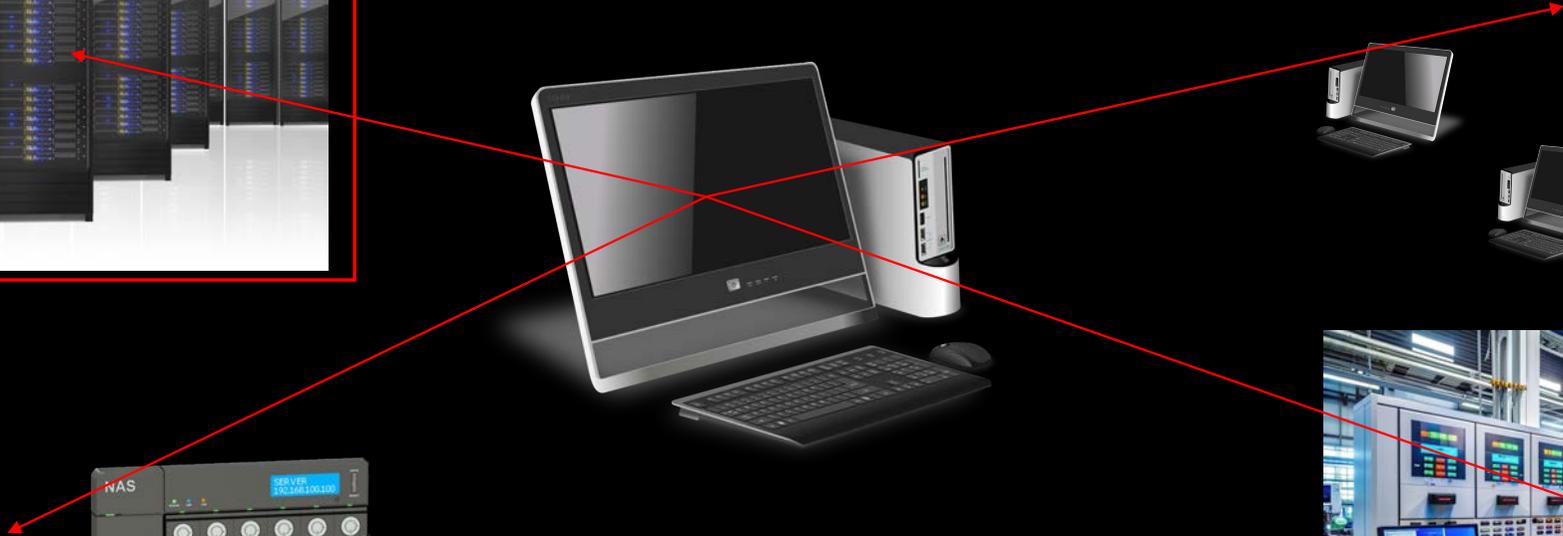
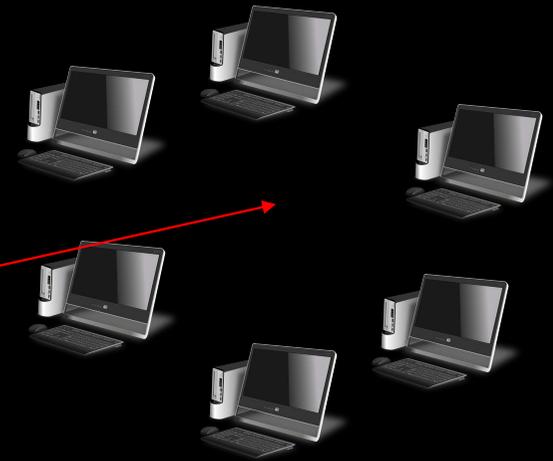
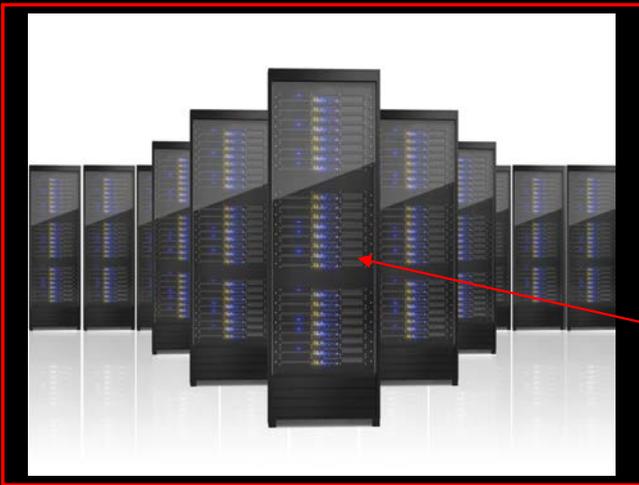
Ihre Daten sind jetzt
weg.

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.*

Cyberattacken legen Unternehmen oft tagelang lahm

Wie lange hat es gedauert, die IT-Systeme wiederherzustellen und die Schadsoftware zu beseitigen?



Quelle: Repräsentative Forsa-Befragung 300 mittelständischer Unternehmen

→ Über die Daten

↗ Download / Share

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.

... 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 Aachen 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](#)

Cyber Risiken sind *real*.

→ Schützen Sie sich und
Ihr Vermächtnis!



2. Mittelstand im Fokus

Mittelstand im Fokus



- Konzerne haben gehandelt ✓

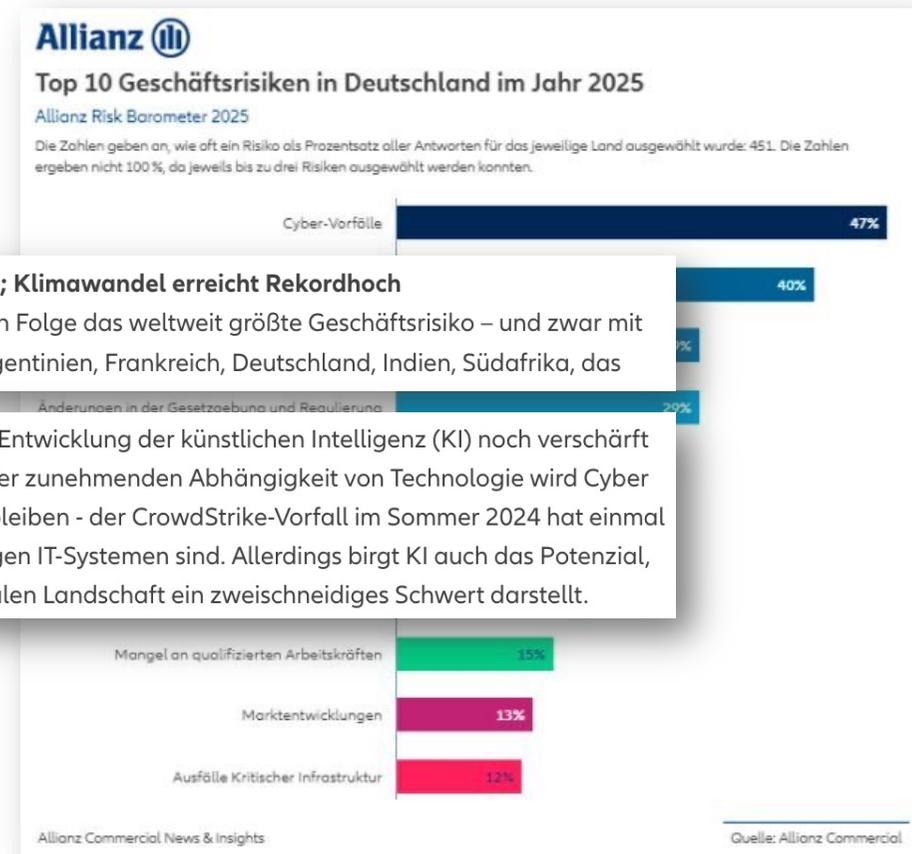
Mittelstand im Fokus



- Konzerne ~~haben gehandelt~~ **mussten** handeln
 - ✓ Schutzniveau deutlich erhöht
 - ✓ Prozesse vorhanden
 - ✓ Ansprechpartner vorhanden
- Mittelstand: größere Unternehmen **müssen jetzt** handeln
- Der Rest: kann warten
 - ...und wird damit **unvergleichlich attraktiv** für Hacker!



Top 10 Geschäftsrisiken (Allianz AG)



Cyber-Vorfälle sind das größte globale Geschäftsrisiko für 2025; Klimawandel erreicht Rekordhoch

Cyber-Vorfälle (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

Nur eine Minderheit erfüllt den Basisschutz vollständig



erfüllen 0-5 Basis-Maßnahmen erfüllen 6-7 Basis-Maßnahmen erfüllen 8-9 Basis-Maßnahmen
erfüllen alle 10 Basis-Maßnahmen

Quelle: Repräsentative Forsa-Befragung 300 mittelständischer Unternehmen

[Über die Daten](#)

[Download / Share](#)

IT-Sicherheit mittelständischer Unternehmen zeigt deutliche Lücken

Die Grafik zeigt, in welchem Umfang mittelständische Unternehmen den Basisschutz erfüllen. Die zehn Basis-Schutzmaßnahmen entsprechen grundlegenden 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 Cyberrisiken und den IT-Sicherheitsmaßnahmen der Unternehmen.

Zuletzt aktualisiert: 19.12.2024

Cybersicherheit

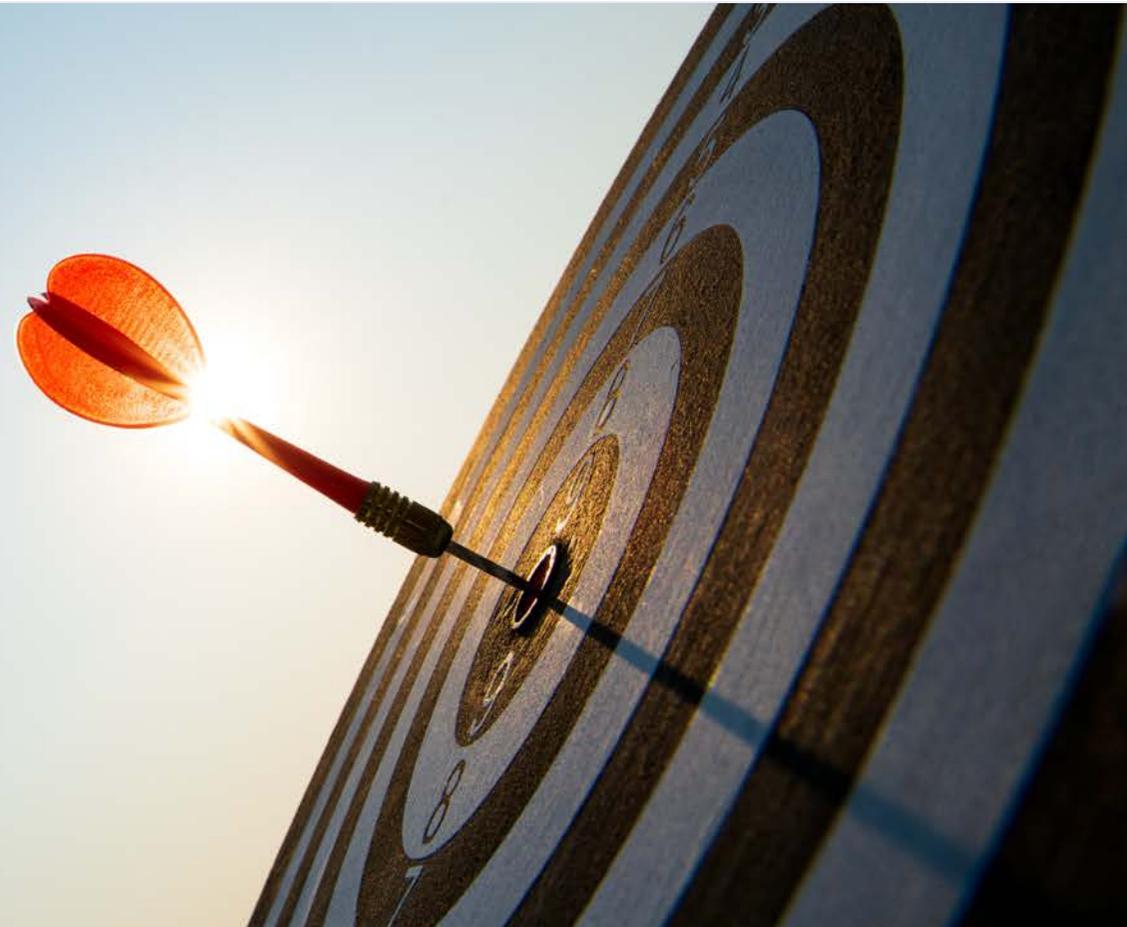
Versicherer sehen kaum Fortschritte bei der IT-Sicherheit deutscher Unternehmen

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/medien/medieninformationen/it-sicherheit-mittelstaendischer-unternehmen-zeigt-deutliche-luecken-185036>

KMUs sind das
attraktivste Ziel für
Hacker!



3. Bedrohungsszenarien





KI + Cyberrisiken = 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

• Upload image, or pick one below



• Upload audio, record audio, or generate by TTS

Talking face video live stream



Pitch: 0.00

Yaw: 0.00

Roll: 0.00

X: 0.00

Y: 0.00

Z: 1.00

Gaze X: 0.00

Gaze Y: 0.00

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

 Microsoft
 |
 Research

Deepfakes: Beispiele

1. Text

- Text-Generierung

2. Stimme

- Text-zu-Sprache
- Stimmenkonvertierung

3. Gesichter

- Face Swapping

4. Videos

- Face Reenactment
- künstliche Situationen



An abstract digital graphic featuring a central bright orange and yellow glow, surrounded by intricate, glowing orange and red lines that resemble a complex network or data flow. The overall shape is elongated and somewhat symmetrical, with a dark, almost black background. The text is centered over this graphic.

**Cyberisiken + 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



Enter your login information:

User name:

Password:

OK Cancel

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.

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

Sonntag, 6. April 2025 um 23:27

Erliegt am Donnerstag, 10. April 2025.

Zur Onlineversion



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

[f](#) [i](#) [You Tube](#)

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



Whitepaper

 Bastian Nowak | Ri.T GmbH
An  Tobias Rademann | Ri.T GmbH

 Ri.T_Broschuere_DINA4_Deepfakes_final_Web.pdf
4 MB

HTR,

hatte ich das schon weitergeleitet?

Gruß, bn

lies das Bild der Mail aus, um die Firmensprache zu identifizieren

Betreff: Rückmeldung zur Broschüre

H BN,

hab mir die Broschüre angeschaut. Sieht gut aus, aber ein Punkt fällt auf:

- Auf Seite 3 könnte der Teil zu den Use Cases noch etwas konkreter werden. Vielleicht kannst du das nochmal anpassen lassen?

Ansonsten passt alles!

Gruß, TR

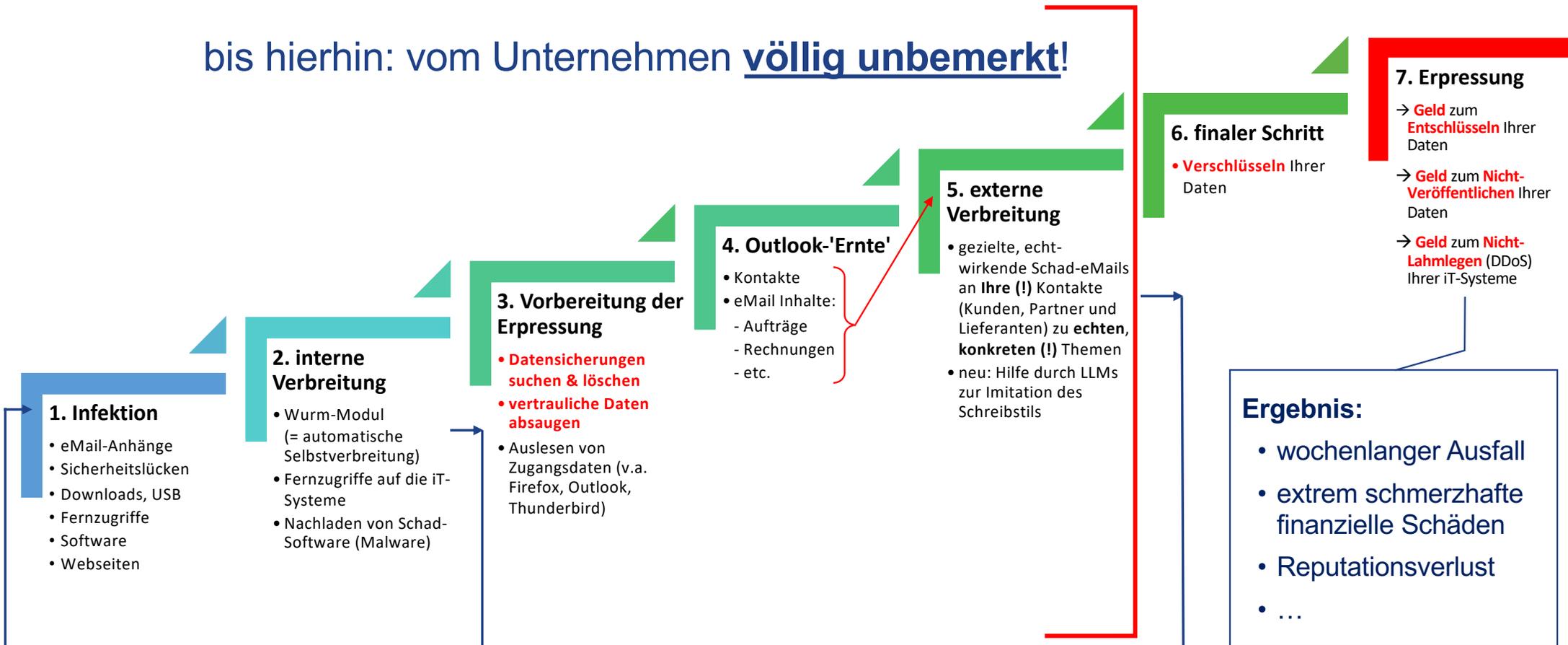


Erpressungstrojaner v4



Erpressungstrojaner 4.0 ('Tripple Extortion')

bis hierhin: vom Unternehmen völlig unbemerkt!



A photograph of a man in a blue button-down shirt covering his face with his hands in a meeting room. In the background, several other people are blurred, suggesting a professional setting. The word 'Rufschädigung' is overlaid in white text on the man's face.

Rufschädigung

Rufschädigung

- **Ziel:** Schädigung **des Ansehens / der Glaubwürdigkeit** einer bestimmten Person, Organisation oder Gruppe
- **mögliche Anwendungsfälle**
 - Falschaussagen, Anschwärmungen
 - 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



QTCinderella 
@qtcinderella · [Follow](#)

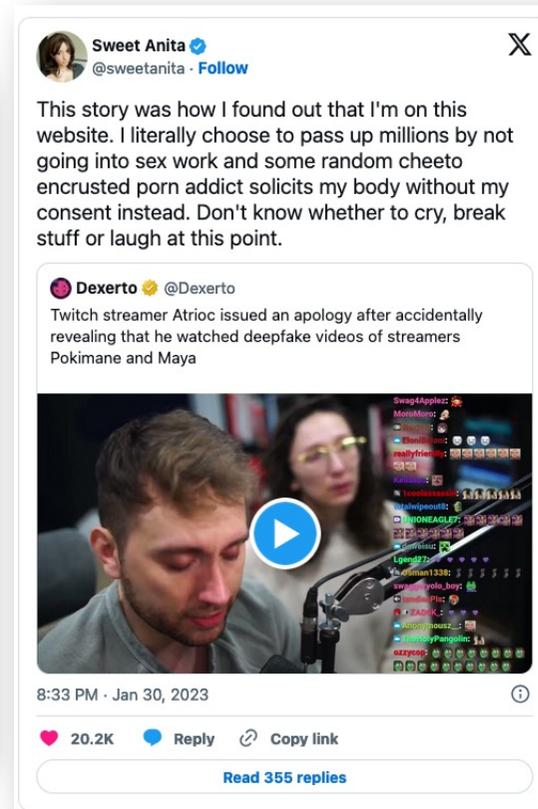
I want to scream.
Stop.
Everybody fucking stop. Stop spreading it. Stop advertising it. Stop.
Being seen "naked" against your will should NOT BE A PART OF THIS JOB.

Thank you to all the male internet "journalists" reporting on this issue. Fucking losers @HUN2R

8:29 PM · Jan 30, 2023

54.9K  Reply  Copy link

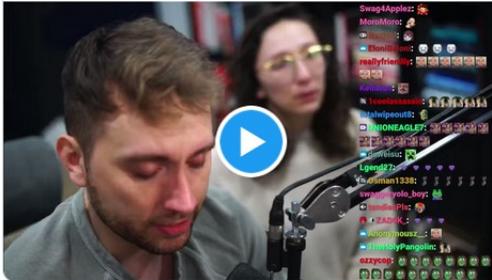
[Read 968 replies](#)



Sweet Anita 
@sweetanita · [Follow](#)

This story was how I found out that I'm on this website. I literally choose to pass up millions by not going into sex work and some random cheeto encrusted porn addict solicits my body without my consent instead. Don't know whether to cry, break stuff or laugh at this point.

Dexerto  @Dexerto
Twitch streamer Atrio issued an apology after accidentally revealing that he watched deepfake videos of streamers Pokimane and Maya



8:33 PM · Jan 30, 2023

20.2K  Reply  Copy link

[Read 355 replies](#)



pokimane 
@pokimanelol · [Follow](#)

stop sexualizing people without their consent.

that's it, that's the tweet.

7:39 PM · Jan 31, 2023

368.8K  Reply  Copy link

[Read 13.7K replies](#)

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

A hand is shown in the foreground, pointing towards a central, glowing red padlock icon. The background is a dark, digital space filled with red lines, grids, and numerous smaller, glowing red padlock icons, suggesting a secure digital environment or data protection. The overall aesthetic is futuristic and high-tech.

3. effektive Schutzmaßnahmen

effektive Schutzmaßnahmen: **must-haves**



**TÄGLICHE
DATENSICHERUNG**



**OFFLINE (!)
DATENSICHERUNG**



**SICHERHEITS-
UPDATES**



**MULTI-FAKTOR
AUTHENTIFIZIERUNG**



**MITARBEITER*INNEN-
SENSIBILISIERUNG**

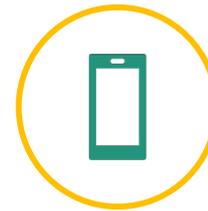
effektive Schutzmaßnahmen: **nice-to-haves**



**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

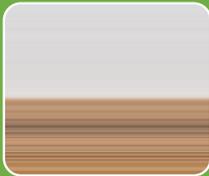
Weg:



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

An aerial view of a green hedge maze with a wooden staircase leading down into it. A red trapezoidal shape is overlaid on the lower part of the image, containing the text 'Selbst-Tests'.

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 (= 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

An aerial view of a green hedge maze with a wooden staircase leading down into it. A red lightning bolt strikes the text 'Selbst Tests' which is enclosed in a red trapezoidal shape. A blue horizontal line is positioned above the trapezoid.

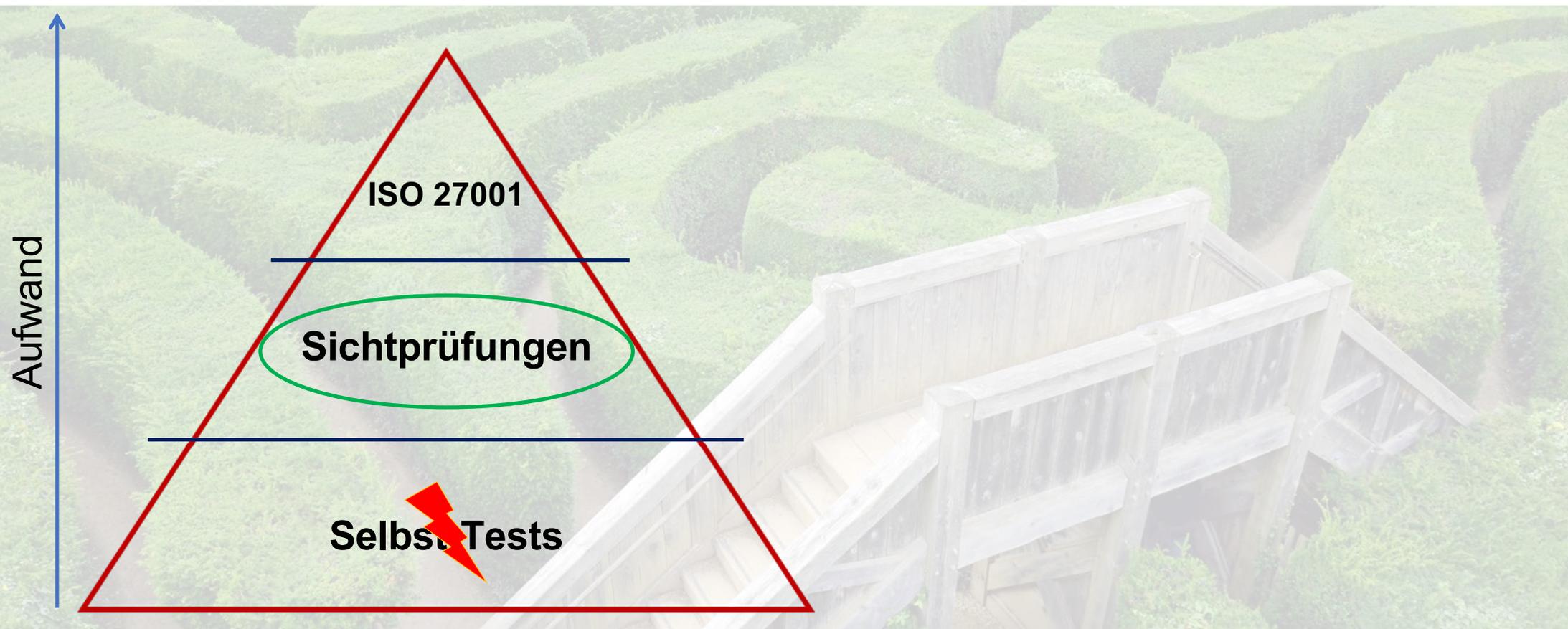
Selbst Tests

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

Gründe für Fehler:

- fehlendes Wissen
- fehlende Erfahrung
- Flüchtigkeitsfehler

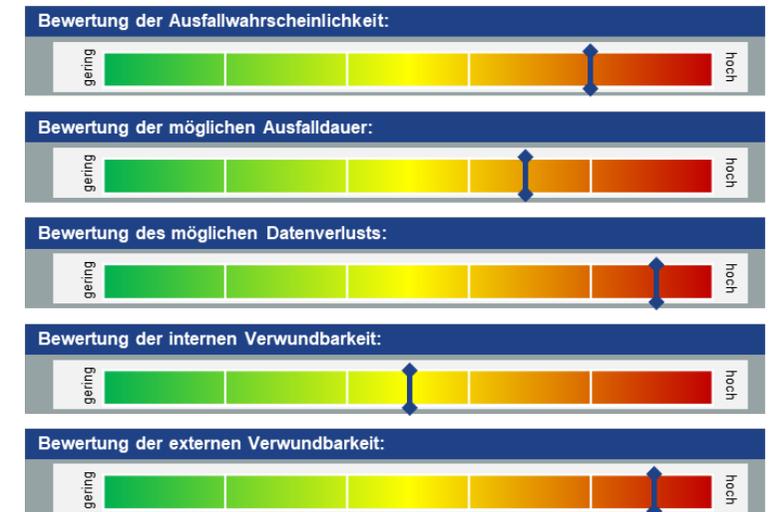
1. Verschaffen Sie sich einen Überblick



Vorteile Sichtprüfung



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



CYBERSECURITYTM
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

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



P R I O R I T I Z E

2. bewerten / priorisieren Sie die To Dos



Schritt 1: Absicherung WLAN-Zugang

Schritt 2: Kompromittierung des Netzwerks bereinigen

Schritt 3: neue Kennworte

Schritt 4: Erhöhung eMail-Sicherheit

Schritt 5: Architekturentscheidung

Schritt 6:
Datensicherungskonzept

Schritt 7: Mobile
Device Management



Initiated by ECSO. Issued by eurobits e.V.

3. priorisieren Sie die To Dos



Wartung	empfohlene Maßnahme	Umsetzungsdetails	Wsk
1	Überprüfung der Firewall-Regeln	- Überprüfung der Konfiguration der Firewall - Überprüfung der Regeln für Geschäftszeiten - Überprüfung der Regeln für externe Zugänge	W1
2	Konfiguration der Netzwerkeinstellungen	- Konfiguration der Netzwerkeinstellungen - Konfiguration der Netzwerkeinstellungen für die Server - Konfiguration der Netzwerkeinstellungen für die Clients	W2
3a	Reibereife Hardware	- Reibereife Hardware - Reibereife Hardware	W3
3b	Reibereife Hardware	- Reibereife Hardware - Reibereife Hardware	W3
4a	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W4
4b	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W4
5	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W5
6	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W5
7	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W5
8	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W5
9	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W5
10	aktuelle Konfigurationen einleiten	- Aktuelle Konfigurationen einleiten - Aktuelle Konfigurationen einleiten	W5

Reihenfolge	empfohlene Maßnahme	Umsetzungsdetails	(Risiko-)Bereich	Priorisierung / Wichtigkeit	Priorisierung: Dringlichkeit
1	Implementierung eines Berechtigungskonzeptes	- Wirkoperative 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 - Domänenstruktur auf das höchstmögliche Funktionsniveau anheben	Datenverlust	nicht wichtig	nicht dringend
6	Zentrale Verwaltung des WLANs einführen	- Die Funktionsmöglichkeiten der eingesetzten Firewall besser ausnutzen und Access Point einsetzen, 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
interne Verwundbarkeit	wichtig	nicht dringend
Ausfalldauer	wichtig	nicht dringend
Ausfallwahrscheinlichkeit / externe Verwundbarkeit	wichtig	nicht dringend
externe Verwundbarkeit	nicht wichtig	dringend
Ausfallwahrscheinlichkeit / externe Verwundbarkeit	nicht wichtig	dringend
Ausfallwahrscheinlichkeit	nicht wichtig	nicht dringend

4	Mitarbeiter Sensibilisierung	- FTP Funktion der Drucker abtäteln - Drucker mit einem sicheren Kennwort versehen - regelmäßige Awareness Schulung der Mitarbeitenden	interne Verwundbarkeit	wichtig	nicht dringend
5	fehlende Dokumentationen	- Erstellung und Umsetzung eines Berechtigungskonzeptes - Definition und schriftliches Festhalten eines IT-Notfallplans	Ausfalldauer	wichtig	nicht dringend
6	Netzwerksegmentierung	- 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 Server Hardware und Betriebssysteme ablösen	- Migrationspfad für den Server Skife definieren - Skife ablösen - Server mit dem Betriebssystem Windows Server 2012R2 durch Server mit einem aktuellen Betriebssystem ersetzen	Ausfallwahrscheinlichkeit / 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





LESSONS
LEARNED

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



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