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

Deepfakes: Die neue Bedrohung

Vortrag im Rahmen des Events 'Cybersicherheit für den Mittelstand: Deepfakes, Angriffe & Prävention'

Tobias Rademann

30. Oktober 2025

ARUP

ARUP

- ✓ multinationales Ingenieurbüro, Hauptsitz in London
- ✓ 17.000 Mitarbeiter in über 90 Büros
- ✓ Umsatz: US$ 1,9 Mrd.

ARUP Deepfake-Cyberangriff

- **Ort:** Hongkonger Niederlassung
- **Kanal:** eMail von Vorgesetztem aus Großbritannien
- **Auftrag:** "vertrauliche Transaktion"
- **Verdacht:** klassische Phishing eMail

- **dann:** Videoanruf mit mehreren Kollegen (u.a. CFO)

  → **alle (!) Deepfakes!**
- **Auftrag:** Überweisung von US$ 25 Mio. in 12 Transaktionen
- **nach Überweisung:** Anruf in Zentrale…

Nicht relevant für Sie, weil…

… Sie zu klein sind?

eine sehr ernst-gemeinte Frage

Würden Sie bewusst
Ihre **Zugangsdaten** oder andere **Interna**
an Dritte weitergeben?

Betreff: Vertraulich - Ihre Aufnahmen vom 15.10.2025

Sehr geehrte/r [Name Mitarbeiter*in],

wir haben kompromittierendes Videomaterial von Ihnen erstellt, das Sie in eindeutigen Situationen zeigt. Die angehängten Screenshots sind nur eine kleine Kostprobe - das vollständige 12-minütige Video zeigt deutlich mehr.

Durch modernste KI-Technologie ist dieses Material von echten Aufnahmen nicht zu unterscheiden. Ihre Kollegen, Familie und Vorgesetzten werden keinen Zweifel an der Echtheit haben.

Was wir haben:

- HD-Videomaterial (1920x1080) mit Ihrem Gesicht
- Ihre Stimme (synthetisiert aus LinkedIn-Videos)
- Metadaten die "beweisen", dass es am [Datum] aufgenommen wurde

Unsere Forderung ist einfach: Sie loggen sich HEUTE bis 18:00 Uhr von Ihrem Heimarbeitsplatz ins Firmennetzwerk ein und laden folgende Dateien herunter:

- Kundendatenbank
- Aktuelle Projektübersicht
- VPN-Zugangsdaten für externe Mitarbeiter

Alternativ: 5.000€ in Bitcoin an [Wallet-Adresse]

Bei Nicht-Erfüllung:

- Versand an alle 847 LinkedIn-Kontakte
- Upload auf einschlägige Websites mit Ihrem vollen Namen
- E-Mail an personalleitung@[ihrfirma].de

Sie haben 24 Stunden. Keine Polizei, keine IT-Abteilung. Wir beobachten Ihre Aktivitäten.

mögliche Multiplikatoren

Stellen Sie sich vor,

- das Foto zeigt: **Arbeitskolleg*in**
  Mitglied Ihres Sportvereins
  Nachbar*in

- Ihre SoMe-Profile / die Ihres Umfelds zeigen, dass es in Ihrem privaten Umfeld gerade Spannungen gibt

- es gibt einen fake SoMe-Account mit Likes zu Ihrem Account und mit Inhalten rund um die (Fake-)Fotos / Videos

eine sehr ernst-gemeinte Frage

Würden Sie bewusst
Ihre **Zugangsdaten** oder andere **Interna**
an Dritte weitergeben?

Deepfakes und iT-Sicherheit

- ⚠ **alle Mitarbeiter*innen = realistische Opfer**
- ⚠ neue Bedrohungslage
- ⚠ kaum (technisch) erkennbar
- ⚠ kaum (technischer) Schutz möglich

Deepfakes und iT-Sicherheit

Deutschland ist **europäischer Spitzenreiter** bei den **Wachstumsraten**

Deepfakes und iT-Sicherheit


STEP
BY
STEP

Agenda

1. *Sensibilisierung*
2. Was sind Deepfakes
3. Bedrohungsszenarien
4. Schutzmöglichkeiten
5. Résumée

Kurzprofil: R.iT GmbH

- **Ausrichtung:** iT-Unternehmensberatung
- **Kernthema:** Digitale Transformation Ihres Unternehmens
  - ✓ Managementberatung (Mindset, Daten/KI)
  - ✓ **iT-Sicherheit**
  - ✓ iT-gestützte Geschäftsprozessoptimierung
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte:** **Zentrale:** **Bochum**
  Region Süd: Cham
  Region Nord: Bad Schwartau
- **Engagement:** DIHK IKT-Ausschuss
  eurobits e.V.
- **Auszeichnungen:**

I. Deepfakes: Hintergrundinformationen

Deepfakes

Deep
→ deep learning

+

Fake
→ Täuschung / Illusion

→ **Ziel:** Erstellung **künstlicher** (von GenAI erschaffener) Medieninhalte, die **täuschend echt wirken** und kaum erkannt werden können.

Deepfakes

Deepfakes: Beispiele

1. **Text**
   - Text-Generierung

Basierend auf deinem Schreibstil erstelle ich dir eine authentische E-Mail:

Betreff: Überweisung während meines Urlaubs

Von: Tobias Rademann | R.iT GmbH
An: Bastian Nowak | R.iT GmbH

HBN,

könnten Sie bitte während meines Urlaubs folgende Überweisung veranlassen:

Betrag: € 5.000,00
Empfänger: Maximilian Muster
IBAN: DE65 7814 0112 0235 8166 00

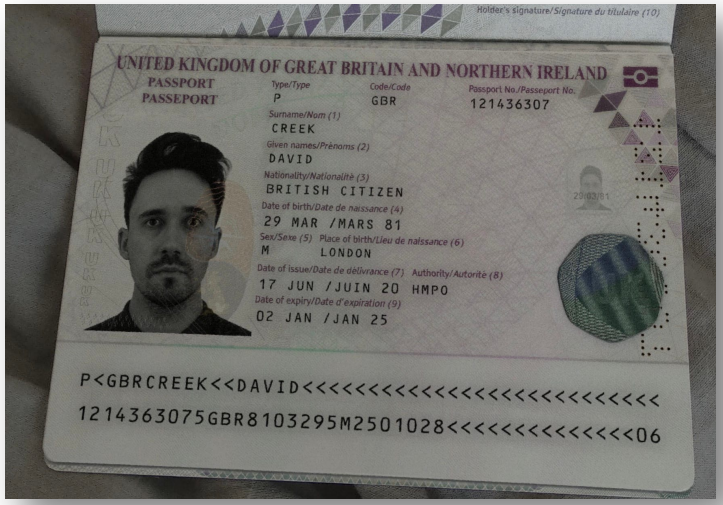
Hintergrund können wir gern nach meiner Rückkehr im JF besprechen, falls erforderlich.

Vielen Dank vorab!

vG
Ihr
tr.

Deepfakes: Beispiele

1. *Text*
   - *Text-Generierung*
2. **Dokumente**
   - Ausweisdokumente
   - Finanzdokumente
   - Zertifikate/Nachweise



Quelle: https://www.404media.co/onlyfake-neural-network-fake-id-site-goes-dark-after-404-media-investigation/

Quelle: https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

Deepfakes: Beispiele

1. ***Text***
   - *Text-Generierung*
2. ***Dokumente***
   - *Ausweisdokumente*
   - *Finanzdokumente*
   - *Zertifikate/Nachweise*
3. **Stimme**
   - Text-zu-Sprache
   - Stimmenkonvertierung

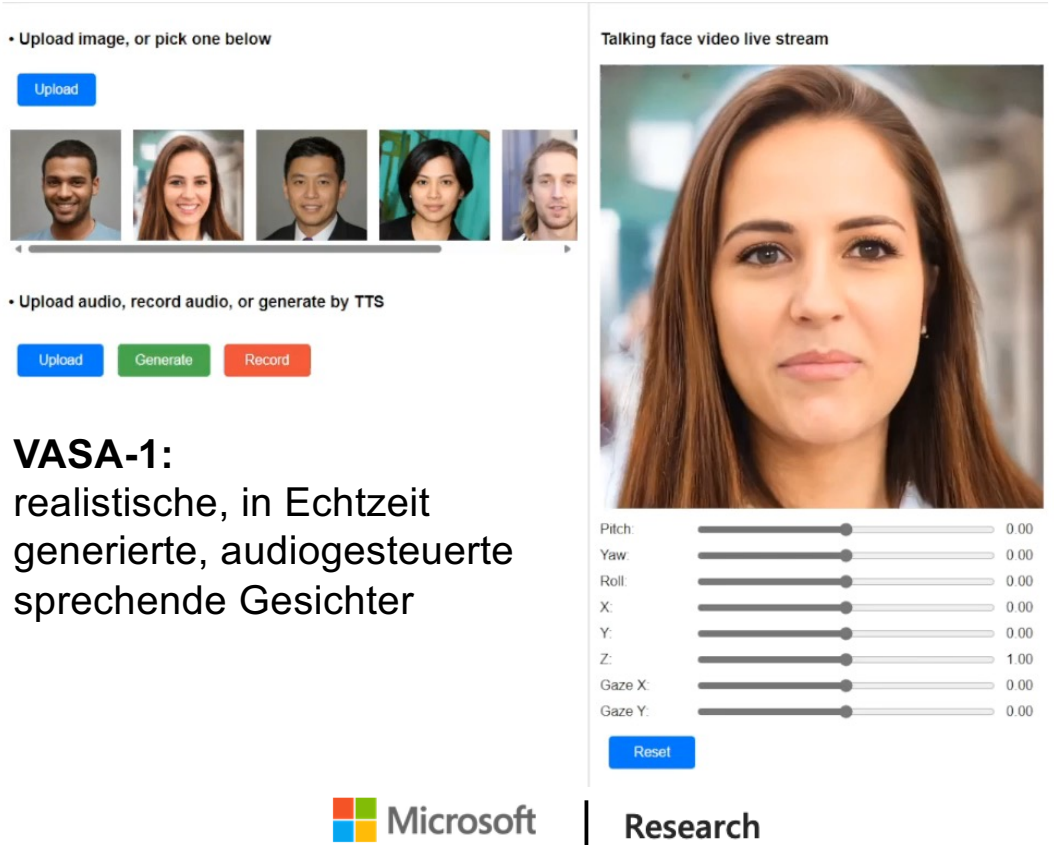
derzeit: Nr. 1 Angriffsart!

Deepfakes: Beispiele

1. ***Text***
   - *Text-Generierung*
2. ***Dokumente***
   - *Ausweisdokumente*
   - *Finanzdokumente*
   - *Zertifikate/Nachweise*
3. ***Stimme***
   - *Text-zu-Sprache*
   - *Stimmenkonvertierung*
4. **Fotos: Gesichter**
   - Face Swapping

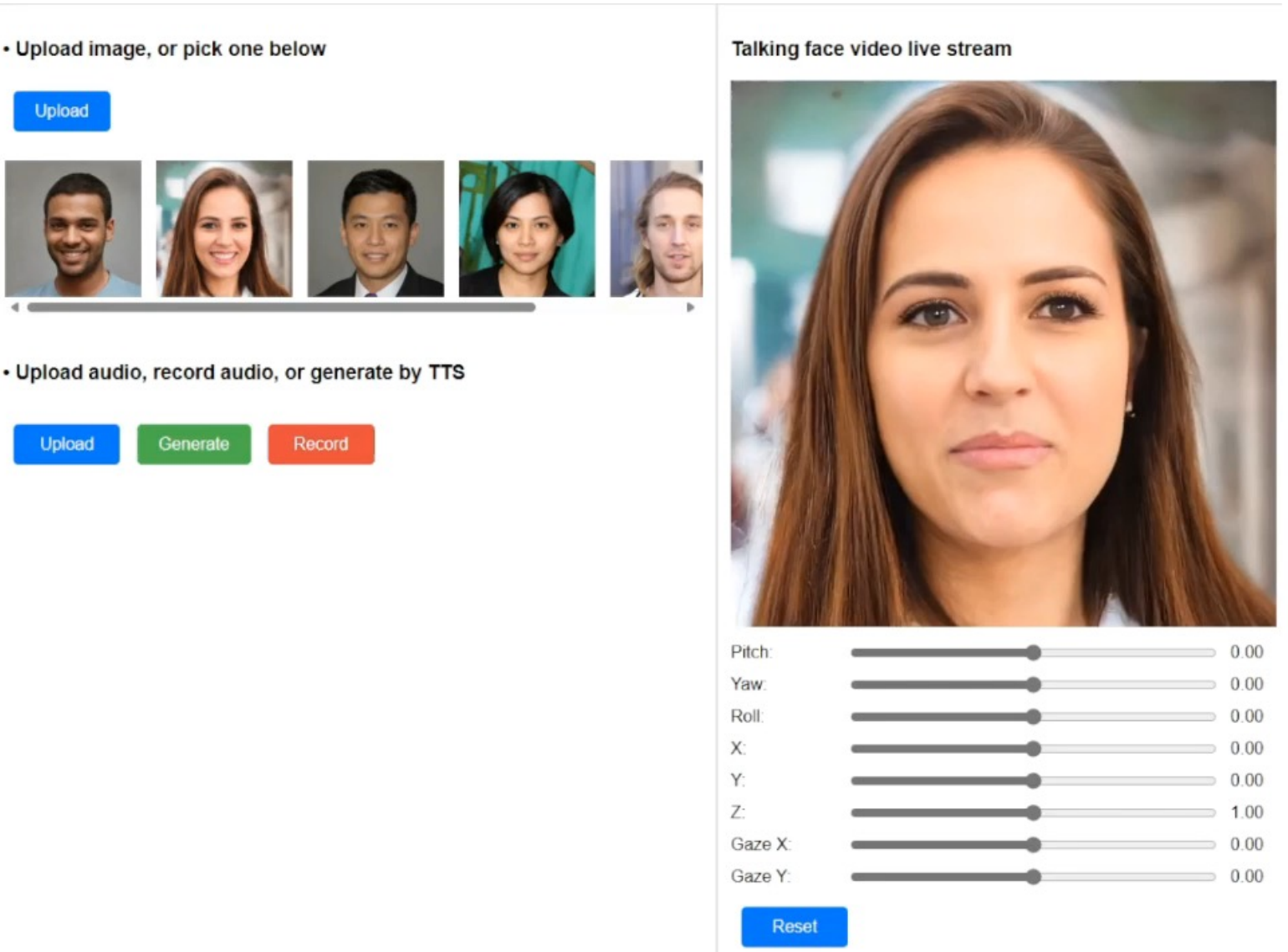
Deepfakes: Beispiele

1. ***Text***
   - *Text-Generierung*
2. ***Dokumente***
   - *Ausweisdokumente*
   - *Finanzdokumente*
   - *Zertifikate/Nachweise*
3. ***Stimme***
   - *Text-zu-Sprache*
   - *Stimmenkonvertierung*
4. ***Fotos: Gesichter***
   - *Face Swapping*
5. **Videos**
   - Face Reenactment



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

Microsoft | Research



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

Microsoft | Research

Deepfakes: Beispiele

1. ***Text***
   - *Text-Generierung*
2. ***Dokumente***
   - *Ausweisdokumente*
   - *Finanzdokumente*
   - *Zertifikate/Nachweise*
3. ***Stimme***
   - *Text-zu-Sprache*
   - *Stimmenkonvertierung*
4. ***Gesichter***
   - *Face Swapping*
5. **Videos**
   - *Face Reenactment*
   - **künstliche Situationen**

Deepfakes: Beispiele

1. ***Text***
   - *Text-Generierung*
2. ***Dokumente***
   - *Ausweisdokumente*
   - *Finanzdokumente*
   - *Zertifikate/Nachweise*
3. ***Stimme***
   - *Text-zu-Sprache*
   - *Stimmenkonvertierung*
4. ***Gesichter***
   - *Face Swapping*
5. **Videos**
   - *Face Reenactment*
   - *künstliche Situationen*
   - **künstliche Identitäten**

Robin Sage is a fictional American cyber threat analyst. She was created in December 2009 by Thomas Ryan, a security specialist and white hat hacker from New York City. Her name was taken from a training exercise of United States Army Special Forces.[1]

Fictional biography [edit]

According to Sage's social networking profiles, she is a 25-year-old "cyber threat analyst" at the Naval Network Warfare Command in Norfolk, Virginia. She graduated from MIT and allegedly had 10 years of work experience, despite her young age.[2] Ryan created several accounts under the name Sage on popular social networks like Facebook, LinkedIn, Twitter etc. and used those profiles to contact nearly 300 people, most of them security specialists, military personnel, staff at intelligence agencies and defense contractors.[1] Her pictures were taken from a pornography-related website in order to attract more attention.[2]

Despite the fake profile and no other real-life information, Sage was offered consulting work with notable companies Google and Lockheed Martin.[2] She also received dinner invitations from several male contacts.[1]

"Robin Sage" as she appeared on social networking pages.

Deepfakes: Beispiele

1. ***Text***
   - *Text-Generierung*
2. ***Dokumente***
   - *Ausweisdokumente*
   - *Finanzdokumente*
   - *Zertifikate/Nachweise*
3. ***Stimme***
   - *Text-zu-Sprache*
   - *Stimmenkonvertierung*
4. ***Gesichter***
   - *Face Swapping*
5. ***Videos***
   - *Face Reenactment*
   - *künstliche Situationen*
   - *künstliche Identitäten*

= Medieninhalte

Deepfakes: Status Quo

Erstellung

- dauert wenige Minuten
- (fast) kostenlos
- kaum technisches Wissen

Erkennung

- technisch + organisatorisch möglich
- hält nicht Schritt
- zudem: nur 22% der Unternehmen nutzen Schutzmaßnahmen

Schäden

- 40 Mrd. US$ bis 2027
- durchschn. Schadenhöhe: € 350.000 - € 500.000

II. Bedrohungsszenarien

II. Bedrohungsszenarien

- Desinformationen
- Rufschädigung
- Erpressung
- CEO-Fraud
- Phishing

II. Bedrohungsszenarien

- *Desinformationen*
- *Rufschädigung*
- **Erpressung**
- **CEO-Fraud**
- **Phishing**

Erpressung (+ Rufschädigung)

Erpressung (+ Rufschädigung)

- **Ziel:** Erpressung von **Geld** oder **sensiblen Informationen / Zugängen** einzelner Individuen (seltener: Unternehmen)
- **mögliche Anwendungsfälle + Beispiele**
  - falsche Aussagen / Anschwärzungen
  - kompromittierende oder kontroverse Situation
  - Ereignis, das nicht existiert oder anders abgelaufen ist
  - falsche Beweise in (Gerichts-)Verfahren
  - die schlichte Behauptung, vorgelegte Beweise seien Deepfakes
- **Achtung**
  - **alle Mitarbeiter*innen mögliche Erpressungsziele**
  - Erpressungsangriffe i.d.R. **'nur' Vorstufe / Einstieg**


CEO-Fraud

CEO-Fraud / Chef-Betrug

- **Ziel:** Veranlassung von Überweisungen > € x00.000,00
- **mögliche Anwendungsfälle**
  - *bisher: eMails, Aufbau von Druck, Einbezug unbekannter Autoritätspersonen*
  - neu: Deepfakes von **Stimmen und Videos bekannter (!), entsprechend befugter Entscheider*innen**
- **Beispiele**
  - s.o.
- **Achtung**
  - hohe Schadenssummen

Phishing / Social Engineering

Phishing / Social Engineering

- **Ziel:** Erlangung sensibler Informationen (→ Emotionen, Neugierde)
  Herunterladen von Schadsoftware
- **mögliche Anwendungsfälle**
  - ! neue Dimension: → **echt-wirkende Formulierungen & Medieninhalte vertrauenswürdiger Personen**
- **Achtung**
  - **alle Mitarbeiter*innen mögliche Ziele**
  - Phishing / Social Engineering i.d.R. **'nur' Vorstufe / Einstieg**

IV. Schutzmaßnahmen

Schutzmaßnahmen

Deepfakes = ***'nur'*** eine ***weitere*** Bedrohungsart
= **verfeinerte Varianten** bekannter Angriffsszenarien

→ **alle bisherigen Schutzmaßnahmen weiterhin sinnvoll!**

Schutzmaßnahmen: **3-Säulen-Ansatz**

- **40% Prozesse**
  - Rückruf über alternativen Kommunikationskanal
  - Vier-Augen-Prinzip
  - Nutzung von Code-Wörtern
  - Incident Response Plan mit definierten Eskalationsstufen
- **30% Technologie**
  - Multi-Faktor-Authentifizierung (MFA) organisationsweit
  - Deepfake-Erkennungstools (z.B. Reality Defender, Pindrop Pulse)
  - verhaltensbasierte Biometrie
- **30% Menschen**
  - rollenspezifisches Awareness-Training
  - vierteljährliche Tabletop-Übungen
  - 'Vertraue nichts, verifiziere alles'-Kultur ('Zero Trust')

Schutzmaßnahmen: **3-Säulen-Ansatz**

- **40% Prozesse**
  - Rückruf über alternativen Kommunikationskanal
  - Vier-Augen-Prinzip
  - Nutzung von Code-Wörtern
  - Incident Response Plan mit definierten Eskalationsstufen
- **30% Technologie**
  - Multi-Faktor-Authentifizierung (MFA) organisationsweit
  - Deepfake-Erkennungstools
  - verhaltensbasierte Biometrie
- **30% Menschen**
  - rollenspezifisches Awareness-Training
  - vierteljährliche Tabletop-Übungen
  - 'Vertraue nichts, verifiziere alles'-Kultur ('Zero Trust')

Wirkung:

60-70% Risikoreduktion

ROI:

Ein verhinderter Vorfall (⌀ € 350.000) rechtfertigt Jahresinvestition.

Schutzmaßnahmen: Quick-Wins

Sofortmaßnahmen (Woche 1-4, € 0 - € 5.000)

- ✓ Rückruf-Protokolle etablieren
- ✓ Multi-Faktor-Authentifizierung nutzen
- ✓ Mitarbeiter sensibilisieren
- ✓ Routinen & Kanäle zur Vorfallsmeldung

Fazit / Ausblick & Diskussion

Résumée

- **2025: DF theoretische Gefahr → existentielle Bedrohung**
- Erstellung: immer leichter
- Erkennung: schwer möglich, v.a. Implementierung…
- plötzlich alle Mitarbeiter*innen = Angriffsziele

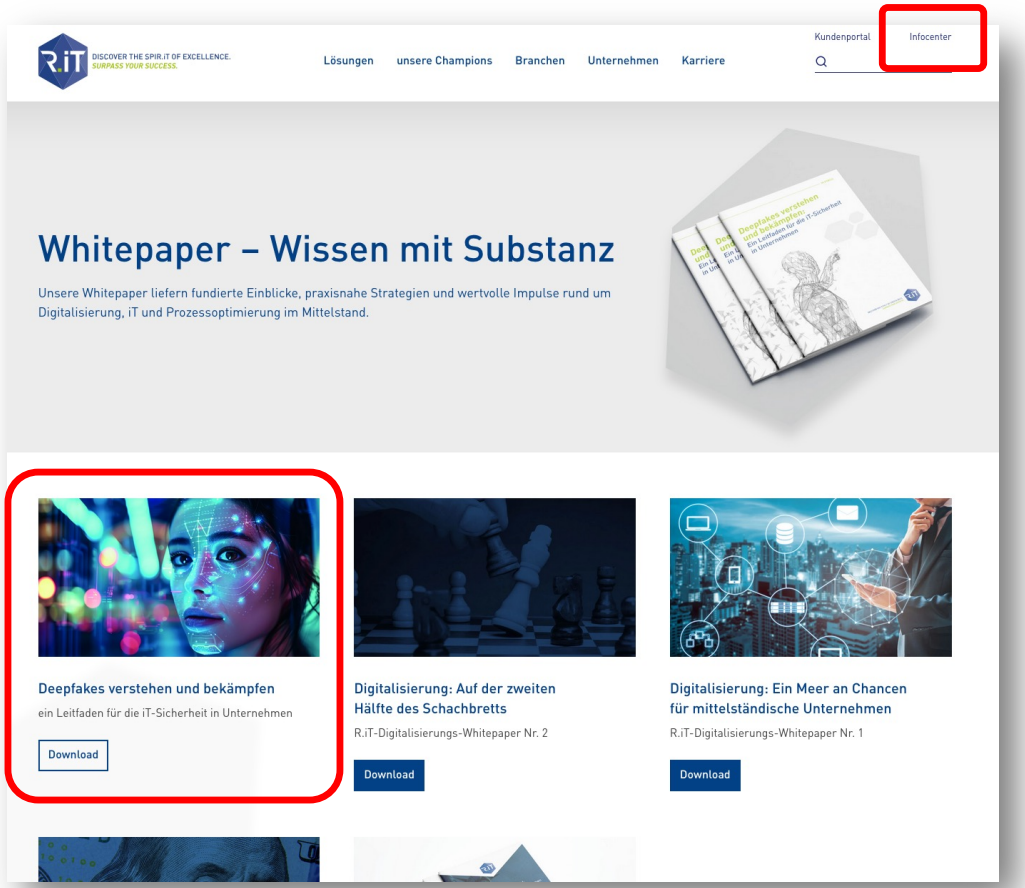
  → Schäden nehmen fast exponentiell zu
- 2023/24:
  27% der Cyberangriffe auf Führungskräfte = KI-gestützte DF-Angriffe
- Mittelstand = primäres Ziel

→ schützen Sie sich vor dieser neuen Bedrohung

weitere Informationen

R.iT Deepfake-Whitepaper

– online: www.RiT.de
→ Infocenter / Whitepaper



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.

R.iT GmbH • www.RiT.de
Zentrale: Lise-Meitner-Allee 37, 44801 Bochum
Tel.: (0234) 43 88 00-0, Fax: -29
NL Süd: Rodinger Straße 15, 93413 Cham
Tel.: (09971) 806 29-0, Fax: -29
NL Nord: Tremskamp 5, 23611 Bad Schwartau
Tel.: (0451) 203 68-500, Fax: -499
eMail: **Tobias.Rademann@RiT.de**