// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

Deepfake-Angriff auf KMU erkennen und abwehren

Deepfake-Betrug trifft auch KMU in Österreich. Wie CEO-Fraud-Angriffe ablaufen, woran Sie Fakes erkennen und welche Sofortmaßnahmen ohne IT-Budget helfen.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
22. Juni 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/deepfake-angriff-kmu-oesterreich-erkennen/

Eine Buchhalterin in einem Grazer Handelsbetrieb erhält eine E-Mail von einem bekannten Lieferanten. Fehlerfreies Deutsch, der gewohnte Ton, Bezug auf eine offene Rechnung und ein laufendes Projekt. Nur eine Sache ist neu: Die Bankverbindung habe sich geändert, bitte die nächste Zahlung auf das neue Konto. Keine Tippfehler, keine holprigen Formulierungen — nichts von dem, woran man Phishing früher erkannt hat. Die Mail ist gefälscht. Das Postfach des Lieferanten wurde übernommen oder die Domain täuschend echt nachgebaut, und eine generative KI hat den Rest geschrieben.

Das ist das Alltagsgesicht KI-gestützten Betrugs — deutlich häufiger als die dramatische Variante mit geklonter Stimme oder gefälschtem Videoanruf. Beides existiert. Aber für ein typisches KMU liegt das realistische, häufige Risiko im Text: in hochüberzeugenden E-Mails. Stimm- und Video-Deepfakes sind der aufwändigere Rand des Spektrums — technisch möglich, zunehmend zugänglich, aber (noch) größeren Summen und Zielen vorbehalten.

Dieser Artikel ordnet das ehrlich ein: was ein Deepfake wirklich ist (und was nicht), wo das echte Risiko für KMU liegt, woran Sie die Muster erkennen, was rechtlich nach österreichischem Recht gilt — und welche Maßnahmen Sie noch diese Woche einführen können, ohne IT-Spezialist zu sein. Ein Gedanke zieht sich durch: Die Technik variiert, das Betrugsmuster und die Abwehr bleiben gleich.

Was ist ein Deepfake – und was nicht?

Ein **Deepfake** ist ein mit KI erzeugtes oder verändertes synthetisches Medium — Audio, Video oder Bild —, das eine reale Person täuschend echt imitiert. Eine perfekt geschriebene gefälschte E-Mail ist demnach **kein** Deepfake, auch wenn der Begriff umgangssprachlich oft so verwendet wird. Sie ist KI-optimiertes Phishing beziehungsweise Business Email Compromise (BEC).

Diese Unterscheidung ist nicht akademisch. Sie entscheidet darüber, wo Sie Ihre Schutzmaßnahmen ansetzen — und sie hilft, das tatsächliche Risiko realistisch einzuschätzen:

- **KI-optimiertes Phishing / BEC (Text):** hohe Häufigkeit, geringer Aufwand. Die Alltagsbedrohung für KMU.
- **Audio-Deepfake (Stimmklon) für CEO-Fraud:** mittlerer Aufwand, wachsend. Mit wenigen Minuten Ausgangsmaterial klingt ein Anruf wie der echte Chef.
- **Echtzeit-Video-Deepfake in Konferenzen:** geringe Häufigkeit, hoher Aufwand. Meist nur bei großen Summen relevant.

KMU sind aus einem einfachen Grund attraktive Ziele: Entscheidungswege sind kurz, Überweisungen werden oft von einzelnen Personen ausgelöst, und auf LinkedIn oder der Firmenwebsite stehen Fotos, Videos und Informationen zur Führungsebene öffentlich zur Verfügung. Angreifer brauchen davon wenig Material, um eine überzeugende Imitation zu erzeugen — oder einfach nur den Namen eines echten Lieferanten und einer laufenden Rechnung.

Der entscheidende Punkt: Generative KI hat den Text-Angriffen genau die Schwächen genommen, an denen viele Mitarbeitende Betrug bisher erkannt haben. Schlechtes Deutsch, falsche Anrede, holprige Sätze — all das ist weg. Der gesunde Skeptizismus gegenüber „verdächtig aussehenden„ E-Mails schützt nicht mehr, weil die E-Mails nicht mehr verdächtig aussehen.

Die häufigsten Angriffsmuster auf KMU in Österreich

1. KI-optimiertes BEC und Rechnungsbetrug – der häufigste Fall

Hier passiert das Geld am häufigsten. Drei typische Spielarten:

- **Lieferanten- und Rechnungsbetrug:** Angreifer übernehmen das Postfach eines Lieferanten oder bauen dessen Domain nach und schicken eine echt wirkende Rechnung mit geänderter Kontoverbindung. Der Kontext stimmt — eine bestehende Geschäftsbeziehung, eine reale offene Position —, deshalb ist diese Form besonders gefährlich.
- **Chef-Masche per Mail:** Eine gefälschte E-Mail der Geschäftsführung bittet um eine dringende Überweisung, um Gutscheinkäufe oder um die Herausgabe sensibler Daten.
- **Thread-Hijacking:** Angreifer klinken sich in einen echten, laufenden E-Mail-Verlauf ein und antworten aus dem Kontext heraus — schwer zu durchschauen, weil die Vorgeschichte echt ist.

Der Ablauf folgt einem Muster:

1. **Aufklärung:** Öffentlich verfügbare Informationen über Unternehmen, Führung, Lieferanten und laufende Projekte werden gesammelt. KI beschleunigt diese Phase erheblich.
2. **Zugang oder Imitation:** Entweder wird ein echtes Postfach übernommen (oft über Phishing oder schwache Passwörter), oder eine täuschend ähnliche Domain registriert.
3. **Kontextgenaue Nachricht:** Eine generative KI formuliert eine fehlerfreie, personalisierte Mail im passenden Stil.
4. **Druckaufbau:** Dringlichkeit, Vertraulichkeit, ein geändertes Konto — die CEO-Fraud-Logik funktioniert per Mail genauso wie am Telefon.
5. **Zahlung oder Datenabfluss:** Ohne Gegenprüfung wird das Geld auf ein unbekanntes Konto transferiert oder eine sensible Auskunft erteilt.

2. CEO-Fraud per Audio-Deepfake (Telefon)

Aufwändiger, aber wachsend. Mit Audiomaterial von LinkedIn-Videos, Firmenwebseiten oder Interviews wird die Stimme einer Führungskraft geklont. Eine Mitarbeiterin, oft aus Buchhaltung oder Verwaltung, erhält dann einen Anruf, der klingt wie der echte Chef.

Ein viel zitiertes Referenzbeispiel stammt aus dem Jahr 2019: Ein britisches Unternehmen überwies rund 220.000 Euro, nachdem ein Angreifer telefonisch — mit der geklonten Stimme des Konzernchefs — eine dringende Zahlung anwies. Das Bundeskriminalamt Österreich warnt explizit vor dieser Methode.

Wichtig: Der Stimmklon kommt zunehmend in Kombination mit einer gefälschten Mail. Die Stimme dient dann als vermeintliche „Bestätigung" und hebelt genau den Reflex aus, der eigentlich schützen soll — den Rückruf zur Verifizierung. Wenn der Bestätigungsanruf von einer Stimmkopie beantwortet wird, wird die Verifizierung selbst zum Angriffsweg. Deshalb gilt: Rückruf immer an eine intern gespeicherte, bekannte Nummer — niemals an die Nummer aus dem Anruf oder der Mail.

3. Echtzeit-Video-Deepfake in Videokonferenzen

Der seltene Spezialfall. Software, die das Gesicht in laufenden Zoom- oder Teams-Calls ersetzt, ist als virtuelle Kamera verfügbar, der Aufwand aber höher. Für Unternehmen ist dieses Szenario derzeit vor allem bei großen Summen relevant — Angreifer investieren mehr, wenn der Ertrag größer ist. Der Trend zeigt in Richtung Massentauglichkeit, ist dort aber noch nicht angekommen. Wer heute Prozesse aufsetzt, ist auf beide Entwicklungsstufen vorbereitet.

4. Gefälschte Identitätsdokumente und Bewerbungen

Ein wachsender Angriffsvektor im HR-Bereich. KI-generierte Bewerbungsfotos oder -videos ermöglichen es, mit erfundener oder gestohlener Identität eingestellt zu werden. Relevant besonders für KMU, die remote onboarden und Bewerberinnen und Bewerber nie physisch sehen — und die es später mit einem „Mitarbeitenden„ zu tun haben, der nicht die Person ist, für die er sich ausgegeben hat.

Erkennungsmerkmale – woran erkennen Sie den Betrug?

KI-optimierte Mails / BEC erkennen – und warum Lesen allein nicht reicht

Die unbequeme Wahrheit zuerst: Eine gut gemachte KI-Mail können Sie am Inhalt kaum noch zuverlässig enttarnen. Die alten Erkennungsmerkmale sind weg. Die Erkennung verschiebt sich deshalb von „liest sich das verdächtig?“ zu prüfbaren, technischen und prozessualen Signalen:

- **Absenderadresse genau prüfen:** Anzeigename und echte Domain auseinanderhalten. Achten Sie auf Lookalike-Domains (etwa `rn` statt `m`, `.co` statt `.com`) und auf eine abweichende Reply-To-Adresse.
- **Inhaltliche Trigger:** Änderung von Bankdaten, eine neue Kontoverbindung, Dringlichkeit, Bitte um Geheimhaltung, Abweichung vom üblichen Weg.
- **Der einzig verlässliche Filter:** Jede Änderung von Zahlungsdaten und jede ungewöhnliche Zahlungsanweisung wird über einen zweiten, bekannten Kanal bestätigt — niemals über die Kontaktdaten aus der Mail selbst.

Verlassen Sie sich nicht auf „die Mail sieht verdächtig aus„. Sie sieht es nicht mehr.

Audio-Deepfakes erkennen

Kein Stimmklon ist perfekt. Bei genauem Hinhören fallen manchmal auf:

- **Unnatürliche Pausen** oder ungewöhnlich flüssige, roboterhafte Übergänge
- **Fehlendes Umgebungsgeräusch** — eine Person im Büro klingt anders als ein schalltoter KI-Output
- **Leichtes Rauschen oder Artefakte**, besonders bei Konsonanten wie S und T
- **Ungewohnte Wortwahl oder Satzstruktur**, die nicht zum bekannten Sprachstil passt

Verlassen Sie sich aber nicht auf Ihr Gehör — bei guten Klonen ist das unzuverlässig. Wirksam ist der **persönliche Kontrollcheck:** Stellen Sie eine Frage, die nur die echte Person beantworten kann — den Namen des letzten gemeinsamen Mittagessen-Lokals, den internen Projektnamen, den Spitznamen einer Kollegin. Ein Stimmklon kann nicht improvisieren. Noch verlässlicher ist der Rückruf über eine intern gespeicherte Nummer.

Video-Deepfakes erkennen

Ältere und einfachere Modelle hinterlassen visuelle Spuren:

- **Flackernde Lichtkanten** am Gesicht, besonders bei Bewegung
- **Unscharfer Haaransatz** oder unnatürliche Übergänge zwischen Gesicht und Hintergrund
- **Unregelmäßiges oder fehlendes Blinzeln**
- **Zähne und Ohren** werden oft unscharf oder verzerrt dargestellt
- **Hände vor dem Gesicht:** Bitten Sie die Person, kurz die Hand vor die Kamera zu halten oder ein beschriebenes Blatt hochzuhalten. Viele Echtzeit-Systeme versagen hier.

Ein einfacher Test bei Videokonferenzen: „Ich habe gerade einen Verbindungsabbruch — können Sie kurz neu einwählen?“ Viele Deepfake-Setups reagieren auf solche Unterbrechungen auffällig. Aber Vorsicht: Neuere Modelle beheben viele dieser Schwächen. Auch hier schlägt der Prozess die Erkennung.

Kontextuelle Warnsignale – unabhängig von der Technik

Das Betrugsmuster ist verlässlicher erkennbar als die Technik dahinter. Es taucht in der Mail, am Telefon und im Videocall gleichermaßen auf:

- **Ungewöhnliche Dringlichkeit** („das muss in den nächsten 20 Minuten passieren„)
- **Bitte um Geheimhaltung** gegenüber Kolleginnen oder Vorgesetzten
- **Geänderte Bankdaten oder unbekanntes Zielkonto** — oder eine Begründung, warum das normale Konto nicht verwendet werden kann
- **Kommunikationsweg außerhalb der Norm** — jemand, der sonst nie auf diesem Weg Zahlungen anordnet, tut es plötzlich

Diese Muster sind Ihr zuverlässigster Filter — egal, ob die Imitation aus geklonter Stimme, gefälschtem Video oder einer makellosen KI-Mail besteht.

Tools zur Erkennung – ein realistischer Überblick

Zuerst eine wichtige Einordnung: Tools zur Deepfake-Erkennung prüfen synthetische **Medien** (Audio, Video, Bild). Gegen die häufigste Bedrohung — die gefälschte E-Mail — helfen sie nicht. Dort ist die Verteidigung eine andere:

- **E-Mail-Authentifizierung:** SPF, DKIM und vor allem korrekt konfiguriertes DMARC (auf „reject“) erschweren das Fälschen Ihrer Domain erheblich. Große Anbieter erzwingen diese Standards inzwischen ohnehin zunehmend. Das ist die technische Antwort auf Domain-Spoofing.
- **Prozess:** die Verifizierung von Zahlungs- und Bankdatenänderungen über einen bekannten zweiten Kanal.

Für aufgezeichnetes Medienmaterial gibt es Werkzeuge — mit klaren Grenzen:

- **Hive Moderation** bietet einen kostenlosen webbasierten Test für Bilder und Videos. Bei gut produzierten Deepfakes liegt die Treffsicherheit unter unabhängigen Tests aber unter 80 % — brauchbar als zweite Meinung, nicht als alleinige Entscheidungsgrundlage.
- **InVID / WeVerify Browser-Plugin** ist kostenlos und gut geeignet, um Metadaten und Ursprung von Videoclips zu prüfen. Ursprünglich für Journalisten entwickelt, auch für KMU brauchbar.
- **Microsoft Video Authenticator** war eine frühe Lösung, ist aber nicht mehr öffentlich verfügbar. Microsoft bietet Content-Authentifizierung über Azure an — für einzelne Mitarbeitende ohne technischen Hintergrund jedoch nicht zugänglich.
- **Intel FakeCatcher** (Blutfluss-Analyse in Videoframes) ist technisch beeindruckend, aber ein Forschungsprojekt — kein Self-Service-Tool.
- **Sensity AI** richtet sich an Enterprise-Kunden mit entsprechenden Budgets. Für ein KMU unter 50 Mitarbeitenden kein realistischer Einstieg.

Ehrliche Einschätzung: Kein verfügbares Tool erkennt Deepfakes zuverlässig in Echtzeit, und gegen gefälschte Mails helfen sie gar nicht. Der wirksamste Schutz ist ein Prozess, kein Tool — ein Rückruf über eine intern gespeicherte Nummer schlägt jede Software.

Rechtliche Lage in Österreich – was gilt bei einem Vorfall?

Strafrecht (StGB)

Bei KI-gestütztem Betrug greifen mehrere Tatbestände des österreichischen Strafgesetzbuches:

§ 146 StGB (Betrug) ist der zentrale Tatbestand, wenn durch Täuschung ein finanzieller Schaden entsteht. Sowohl gefälschte Zahlungs-Mails als auch Deepfake-gestützter CEO-Fraud fallen in der Regel darunter.

§ 107a StGB (Beharrliche Verfolgung) und **§ 107b StGB (Fortgesetzte Belästigung)** können greifen, wenn Deepfakes gezielt zur Schädigung von Personen eingesetzt werden — etwa bei Fake-Videos gegen Mitarbeitende.

Anzeige erstatten können Sie bei der nächsten Polizeidienststelle oder direkt beim **Bundeskriminalamt Österreich**, das eine Cybercrime-Kompetenzstelle betreibt (bundeskriminalamt.at/cybercrime). Zuständig ist auch das jeweilige Landeskriminalamt (LKA) — die Kontakte finden sich auf der Website des BKA.

DSGVO-Bezug

Wenn ein Angreifer Stimme oder Gesicht einer Person für einen Deepfake verwendet, greift er auf **biometrische Daten** zurück — eine besonders schützenswerte Kategorie nach der DSGVO.

Wenn ein Vorfall personenbezogene Daten von Mitarbeitenden betrifft — etwa weil ein Postfach übernommen wurde und Angreifer auf interne Kommunikationsdaten zugegriffen haben —, besteht unter Umständen eine **Meldepflicht gegenüber der Datenschutzbehörde (DSB)** innerhalb von 72 Stunden. Die Kontaktdaten der DSB finden sich unter dsb.gv.at.

Zur datenschutzkonformen IT-Infrastruktur als struktureller Grundlage finden Sie weiterführende Hinweise in unserem Artikel zur souveränen IT für Firmen.

Wichtig in jedem Fall: **Dokumentieren Sie alles.** Screenshots, Mail-Header, Anrufprotokolle, Zeitstempel — je vollständiger die Dokumentation, desto besser für Anzeige und Versicherungsansprüche.

Versicherung und Haftung

Viele bestehende Cyber-Versicherungspolicen decken Schäden durch Social Engineering nicht automatisch ab — das Thema ist oft jünger als die Vertragstexte. Prüfen Sie Ihre Police konkret auf Formulierungen zu „Social Engineering„ „Fake President“ und „CEO-Fraud„; diese stehen häufig als eigene, separat zu vereinbarende Klausel. Ein kurzes Gespräch mit Ihrem Versicherungsmakler ist hier sinnvoller als eine Selbsteinschätzung.

Sofortmaßnahmen für KMU – was Sie noch diese Woche umsetzen können

Interne Prozesse (kostenlos)

Bankdaten-Änderungen verifizieren — die wichtigste Einzelmaßnahme: Jede Änderung einer Kontoverbindung — ob von einem Lieferanten oder einem anderen Empfänger — wird über einen bekannten, zweiten Kanal bestätigt, bevor die nächste Zahlung erfolgt. Rückruf an die in Ihren Stammdaten gespeicherte Nummer, nicht an die Nummer aus der Mail. Das ist der wirksamste Schutz gegen Rechnungsbetrug.

Vier-Augen-Prinzip bei Überweisungen: Legen Sie fest, dass Zahlungen ab einem Schwellenwert — etwa ab 1.000 € — grundsätzlich von zwei Personen freigegeben werden müssen. Auch dann, wenn die Anweisung scheinbar von der Geschäftsführung kommt.

Rückrufpflicht: Jede ungewöhnliche Zahlungsanweisung — per Mail, Telefon oder Video — wird über eine intern gespeicherte Nummer zurückgerufen. Niemals über die Nummer oder den Kontakt, die im Anruf oder in der Nachricht selbst genannt wurden. Bei Stimmklonen ist genau das entscheidend.

Codewort für sensible Anweisungen: Vereinbaren Sie ein internes Codewort oder ein Bestätigungsritual, das vor einer ungewöhnlichen Zahlung verwendet wird. Intern bekannt, nach außen nicht ableitbar.

Technische Basismaßnahmen

E-Mail-Authentifizierung einrichten oder prüfen: SPF, DKIM und DMARC erschweren das Fälschen Ihrer Domain. Das lässt sich mit Ihrem Provider oder Admin umsetzen und ist die technische Gegenmaßnahme zu Domain-Spoofing.

Postfächer und Zugangsdaten absichern: Die Übernahme eines echten Postfachs ist ein häufiger Einstiegspunkt für BEC. Zwei-Faktor-Authentifizierung auf E-Mail-Konten ist deshalb Pflicht. Schwache oder wiederverwendete Passwörter erleichtern Angreifern die Aufklärung — mehr dazu, wie schnell Passwörter heute geknackt werden, in unserem Artikel Der Algorithmus aus 1991, der heute Ihre Passwörter knackt.

Zoom- und Teams-Einstellungen härten: Warteräume für externe Teilnehmende aktivieren, Meeting-IDs nicht öffentlich teilen, Start-Berechtigungen prüfen.

Öffentliche Videoexposition der Führungsebene reduzieren: Prüfen Sie, wie viel Audio- und Videomaterial von Geschäftsführung und leitenden Mitarbeitenden öffentlich zugänglich ist. Jede Minute Audio ist potenzielles Trainingsmaterial für einen Stimmklon. Was nicht öffentlich sein muss, sollte es nicht sein.

Schulung ohne IT-Vorwissen – eine druckfertige Kurzanleitung

Ein 15-minütiges Team-Briefing reicht als Einstieg.

Die drei Warnsignale, auf die alle achten — egal über welchen Kanal: 1. Ungewöhnliche Dringlichkeit 2. Bitte um Geheimhaltung 3. Geänderte Bankdaten, unbekanntes Konto oder ungewohnter Kommunikationsweg

Entscheidungsbaum für verdächtige Anweisungen:

```
Erhalte ich eine ungewöhnliche Zahlungs- oder Bankdaten-Anweisung
(per Mail, Telefon oder Video)?
  → Ja
    Stimmt eines der drei Warnsignale?
      → Ja oder unsicher
        Bestätigung über bekannten zweiten Kanal
        (Rückruf an intern gespeicherte Nummer)
          → Person/Lieferant bestätigt → Vier-Augen-Freigabe → Zahlung
          → Keine Bestätigung → Zahlung stoppen, Vorfall melden
```

Dieser Ablauf sollte schriftlich festgehalten und für alle zugänglich sein — als Aushang, als PDF oder als kurze interne Richtlinie.

Was tun, wenn es passiert ist? – Erste Schritte nach einem Vorfall

Sofort: Zahlung stoppen. Rufen Sie unmittelbar Ihre Bank an und verlangen Sie einen „Recall" oder „Rückruf der Überweisung„. Je schneller Sie reagieren, desto höher die Chance, dass das Geld noch nicht weitertransferiert wurde. Viele Banken haben dafür einen Notfall-Kontakt außerhalb der Geschäftszeiten.

Anzeige erstatten. Kontaktieren Sie die nächste Polizeidienststelle oder direkt das Bundeskriminalamt Österreich unter bundeskriminalamt.at. Parallel sollten Sie prüfen, ob Shadow AI in Ihrem Unternehmen weitere Einfallstore geschaffen hat. Cybercrime-Fälle werden dort von Spezialistinnen und Spezialisten bearbeitet.

DSB informieren, falls personenbezogene Daten betroffen. War der Angriff mit dem Zugriff auf oder der Verarbeitung von Mitarbeiterdaten verbunden — etwa bei einer Postfachübernahme —, besteht möglicherweise eine Meldepflicht innerhalb von 72 Stunden.

Interne Dokumentation sichern. Mail-Header, Screenshots des Video-Meetings, Anrufprotokolle, Überweisungsbelege, Zeitstempel. Diese Dokumentation ist Grundlage für Anzeige, Versicherungsanspruch und interne Aufarbeitung.

Keine Scham. KI-gestützter Betrug ist kein persönliches Versagen. Angreifer investieren erheblichen Aufwand, um Mitarbeitende zu täuschen — das ist ein gut geplanter Angriff, kein Fehler der betroffenen Person. Wer das intern klar kommuniziert, senkt die Hemmschwelle, Vorfälle sofort zu melden.

Praxis-Tipp: KI-Betrugsschutz als Teil Ihrer IT-Sicherheitsstrategie

Schutz funktioniert nicht als Einzelmaßnahme. Er ist am wirksamsten, wenn er in ein durchdachtes IT-Sicherheitskonzept eingebettet ist — mit klaren Zuständigkeiten, dokumentierten Prozessen und regelmäßiger Überprüfung. Der rote Faden bleibt: Die Technik der Angreifer ändert sich, das Betrugsmuster und die Abwehr nicht.

Wenn Ihr Unternehmen KI-Tools einsetzt, lohnt gleichzeitig die Frage, wie gut Ihre internen Prozesse gegen KI-gestützte Angriffe gewappnet sind. Wer etwa KI-Agenten mit Zugang zu Unternehmensdaten betreibt, sollte prüfen, ob diese Zugriffsrechte klar begrenzt sind. Wer etwa KI-Agenten mit Zugang zu Unternehmensdaten betreibt, sollte prüfen, ob diese Zugriffsrechte klar begrenzt sind — mehr dazu in unserem Artikel zu KI-Workflows mit Unternehmensdaten absichern.

Viele KMU haben keinen klaren Ansprechpartner für die Schnittmenge aus KI-Technologie und IT-Sicherheit. Ein KI-Tool Sicherheitsaudit hilft, systematisch Lücken zu identifizieren. Wer intern niemanden hat, der diese Fragen koordiniert, entdeckt Lücken oft erst dann, wenn ein Angriff sie offenlegt.

Wenn Sie nicht sicher sind, wo Ihr größtes Risiko liegt und welche Maßnahmen für Ihre Betriebsgröße sinnvoll sind, bringt ein kurzes Gespräch mit konkretem Blick auf Ihre Situation mehr als jede Checkliste allein. In einer kostenlosen Potenzialanalyse schauen wir uns gemeinsam an, wo Ihre dringlichsten Lücken liegen — ohne Umwege über allgemeine Empfehlungen.

Nächste Schritte – Ihre Kurzcheckliste auf einen Blick

- [ ] Verifizierung von Bankdaten-Änderungen über bekannten zweiten Kanal schriftlich festlegen
- [ ] Vier-Augen-Prinzip für Überweisungen ab 1.000 € einführen
- [ ] Rückrufpflicht: immer über intern gespeicherte Nummer, nie über die in Mail/Anruf genannte
- [ ] Internes Codewort für sensible Zahlungsanweisungen vereinbaren
- [ ] E-Mail-Authentifizierung (SPF, DKIM, DMARC) einrichten oder prüfen lassen
- [ ] Zwei-Faktor-Authentifizierung auf allen E-Mail-Konten aktivieren
- [ ] Öffentliches Audio-/Videomaterial der Führungsebene prüfen und wo möglich reduzieren
- [ ] Zoom/Teams-Einstellungen härten (Warteraum, Meeting-IDs schützen)
- [ ] 15-minütiges Team-Briefing zu den drei Warnsignalen durchführen
- [ ] Entscheidungsbaum für verdächtige Anweisungen dokumentieren und verteilen
- [ ] Cyber-Versicherungspolice auf Social-Engineering-/CEO-Fraud-Abdeckung prüfen
- [ ] Kontakt des Bundeskriminalamts Cybercrime intern bekannt machen

---

Häufige Fragen zu KI-gestütztem Betrug auf KMU

Ist die gefälschte Mail wirklich gefährlicher als der Deepfake-Anruf?

Für die meisten KMU: ja, in der Häufigkeit. Gefälschte und KI-optimierte Geschäftsmails — Rechnungsbetrug, Chef-Masche, Thread-Hijacking — sind der mit Abstand häufigste und finanziell schwerwiegendste Angriffsweg. Stimm- und Video-Deepfakes existieren und wachsen, sind aber aufwändiger und treffen meist größere Ziele. Die gute Nachricht: Dieselben Prozesse schützen gegen beides.

Wie erkenne ich eine gefälschte Mail, wenn sie keine Tippfehler mehr hat?

Am Inhalt meist gar nicht zuverlässig — genau das ist der Punkt. Prüfen Sie die Absenderdomain genau (Lookalike-Adressen, abweichende Reply-To) und behandeln Sie jede Änderung von Bankdaten als Anlass für eine Rückfrage über einen bekannten zweiten Kanal. Die Verteidigung liegt im Prozess, nicht im genauen Hinsehen.

Kann ein Angriff auch Kleinstunternehmen mit unter 10 Mitarbeitenden treffen?

Ja — gerade sehr kleine Betriebe sind attraktiv. Wenn eine einzelne Person alle Zahlungen auslöst und keine zweite Freigabe nötig ist, reicht eine einzige überzeugende Mail oder ein Anruf. Angreifer wählen nicht nach Unternehmensgröße, sondern nach Aufwand-Ertrag-Verhältnis.

Wie viel kostet der Schutz?

Die wirksamsten Maßnahmen — Prozesse, Bankdaten-Verifizierung, Codewörter, Rückrufpflicht, Vier-Augen-Prinzip — kosten nichts außer Zeit. E-Mail-Authentifizierung und 2FA sind mit überschaubarem Aufwand umsetzbar. Den größten Schutz kaufen Sie nicht, Sie organisieren ihn.

Meine Mitarbeitenden haben bereits Geld überwiesen — gibt es eine Chance, es zurückzubekommen?

Ja, wenn Sie schnell handeln. Viele Banken können Überweisungen zurückrufen, solange das Geld noch nicht weitertransferiert wurde — dieser Zeitraum ist oft kürzer als eine Stunde. Rufen Sie sofort Ihre Bank an, Stichwort „Recall" oder „Rückruf der Überweisung„. Danach parallel die Anzeige beim Bundeskriminalamt, da Strafverfolgungsbehörden unter Umständen Kontensperrungen im Ausland einleiten können.