// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI-generierte E-Mails erkennen & Absender verifizieren

Wie KMU in Österreich KI-Phishing erkennen: SPF, DKIM, DMARC verständlich erklärt plus kostenlose Tools und Mitarbeitertipps.

AUTOR
Strukturaflow IT-Team

VERÖFFENTLICHT
6. August 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/ki-generierte-email-absender-verifizieren-kmu-oesterreich/

Eine E-Mail von Ihrer Hausbank, perfektes Deutsch, Ihr korrekter Name, eine glaubwürdige Signatur — und trotzdem eine Fälschung. Was früher stundenlange manuelle Arbeit erforderte, erledigt ein Sprachmodell heute in Sekunden. Für österreichische KMU ohne eigene IT-Abteilung ist das ein ernstes Problem, das mit der altbekannten Regel „auf Rechtschreibfehler achten" nicht mehr lösbar ist.

Dieser Guide zeigt Ihnen, welche technischen Methoden tatsächlich helfen, wie Sie konkret verdächtige Absender verifizieren und was Ihr Unternehmen mit überschaubarem Aufwand dauerhaft absichert.

Warum KI-generierte Phishing-Mails für KMU heute gefährlicher sind als je zuvor

Klassisches Phishing war erkennbar: holpriges Deutsch, generische Anrede, verdächtige Links mit kyrillischen Zeichen. Diese Mails filtert inzwischen jeder Spamfilter zuverlässig heraus. KI-generierte Phishing-Mails spielen in einer anderen Liga.

Moderne Sprachmodelle produzieren stilistisch unauffällige, grammatikalisch korrekte Texte — angepasst an den Schreibstil der vorgespiegelten Organisation, personalisiert mit öffentlich verfügbaren Informationen aus LinkedIn, der Firmenwebseite oder früheren E-Mails. Laut dem ENISA Threat Landscape 2024 hat die Qualität und Zielgenauigkeit von Phishing-Angriffen durch KI-Unterstützung deutlich zugenommen.

KMU sind aus zwei Gründen besonders betroffen: Sie haben weniger technische Schutzmaßnahmen im Einsatz als Großunternehmen, und sie vertrauen E-Mail als primärem Kommunikationskanal oft unkritisch. Ein einziger erfolgreicher Angriff — etwa eine gefälschte Zahlungsaufforderung vom vermeintlichen Lieferanten — kann existenzielle Folgen haben.

Was KI-gestützte Ransomware für KMU bedeutet, wenn ein Angreifer erst einmal im System ist, beschreibt unser Artikel zu KI-automatisierter Ransomware.

Was beim Absender wirklich zählt - und was nur so aussieht

Anzeigename vs. tatsächliche Absenderadresse

E-Mail-Clients zeigen standardmäßig den Anzeigenamen an — und dieser ist vollständig frei wählbar. Ein Angreifer kann seinen Absender-Anzeigenamen auf „Erste Bank Austria Kundenservice" setzen, während die eigentliche technische Absenderadresse `service@erste-bank-austria-secure.com` lautet — eine Domain, die er selbst registriert hat.

In Outlook blenden Sie die vollständige Absenderadresse ein, indem Sie mit der Maus über den Anzeigenamen fahren oder die Mail öffnen und auf den Namen klicken. In Gmail sehen Sie die Adresse direkt neben dem Namen im Kopfbereich, sobald Sie auf den Pfeil neben „An mich“ klicken. In Apple Mail: Ansicht → Alle Header einblenden.

Gewöhnen Sie sich an: Anzeigename ignorieren, Absenderadresse lesen.

Domain-Spoofing und Look-alike-Domains

Selbst wenn die Absenderadresse offiziell wirkt, lohnt sich ein zweiter Blick auf die Domain. Typische Täuschungsmanöver:

- Buchstabentausch: `strukturaflow.com` vs. `strukturaf1ow.com` (l durch 1 ersetzt)
- Zusätze: `erstebank.at` vs. `erste-bank-sicherheit.at`
- Länderdomain-Wechsel: `bmf.gv.at` vs. `bmf.gov-austria.com`

Die offizielle Domain einer österreichischen Organisation finden Sie über deren Website-Impressum oder über eine WHOIS-Abfrage bei `nic.at` (für .at-Domains) bzw. `whois.domaintools.com`.

Was E-Mail-Header verraten

Hinter jeder E-Mail steckt ein technischer Protokollblock — der Header. Er enthält Informationen, die der Absender nicht fälschen kann, ohne an den E-Mail-Servern zu scheitern.

So öffnen Sie den Header: - **Outlook:** Mail öffnen → Datei → Eigenschaften → „Internetkopfzeilen“ - **Gmail:** Drei Punkte → „Original anzeigen“ - **Apple Mail:** Darstellung → Nachrichtenkopfzeilen → Alle

Die wichtigsten Felder: - **Received:** Zeigt den Weg der Mail durch verschiedene Server — von unten nach oben lesen - **Return-Path:** Wohin gehen Rückantworten? Weicht diese Adresse vom sichtbaren Absender ab, ist das ein Warnsignal - **Authentication-Results:** Hier stehen die Ergebnisse der technischen Prüfung: `spf=pass`, `dkim=pass`, `dmarc=pass` — oder eben `fail`

Die technischen Schutzprotokolle - verständlich erklärt

SPF - wer darf von dieser Domain senden?

SPF (Sender Policy Framework) legt in einem DNS-Eintrag fest, welche Mailserver berechtigt sind, E-Mails im Namen Ihrer Domain zu versenden. Empfänger-Server prüfen das automatisch: Kommt eine Mail von einem nicht autorisierten Server, schlägt SPF fehl.

Konkretes Beispiel: Ihre Domain lautet `meinbuero.at`. Ihr SPF-Eintrag erlaubt nur Mails über Microsoft 365. Eine gefälschte Mail, die über einen anderen Server gesendet wird, fällt bei der SPF-Prüfung durch.

Ihren eigenen SPF-Eintrag prüfen Sie kostenlos mit MXToolbox: Domain eingeben, „SPF Record Lookup“ auswählen — fertig.

DKIM - die digitale Unterschrift

DKIM (DomainKeys Identified Mail) funktioniert wie ein Siegel auf einem Brief. Beim Versand signiert Ihr Mailserver die E-Mail mit einem privaten Schlüssel. Der Empfänger-Server verifiziert diese Signatur mit dem öffentlichen Schlüssel, den er in Ihren DNS-Einträgen findet.

Was DKIM schützt: Manipulation des Mailinhalts auf dem Transportweg. Was es nicht schützt: das Registrieren einer ähnlichen Domain durch Angreifer. DKIM bestätigt nur, dass die Mail tatsächlich von der angegebenen Domain stammt — nicht, dass diese Domain vertrauenswürdig ist.

DMARC - die Richtlinie, die alles zusammenbringt

DMARC (Domain-based Message Authentication, Reporting & Conformance) verbindet SPF und DKIM zu einer Richtlinie und teilt Empfänger-Servern mit, was mit Mails passieren soll, die beide Prüfungen nicht bestehen: Zustellen, in Quarantäne verschieben oder ablehnen.

Für KMU empfehlen wir, die DMARC-Richtlinie mittelfristig auf `p=reject` zu setzen. Das bedeutet: E-Mails, die Ihre Domain vortäuschen aber SPF oder DKIM nicht bestehen, werden abgelehnt — nicht nur markiert.

Zudem liefert DMARC regelmäßige Berichte darüber, wer im Namen Ihrer Domain sendet. Das ist wertvoll, um unbekannte legitime Sendequellen (Newsletter-Tools, Buchhaltungssoftware) zu identifizieren, bevor Sie auf `reject` umstellen.

Kostenlose DMARC-Prüfung und einfaches Monitoring bieten EasyDMARC und dmarcian.com — beide haben brauchbare kostenlose Tiers für kleine Teams.

Ehrliche Einschätzung: SPF, DKIM und DMARC schützen Ihre eigene Domain vor Missbrauch. Sie verhindern nicht, dass ein Angreifer eine ähnlich klingende Domain registriert und von dort aus schreibt. Dafür braucht es die menschliche Prüfung.

KI-spezifische Erkennungsmethoden - was jetzt neu dazukommt

Sprachmodell-Fingerprinting (einfach erklärt)

Tools wie GPTZero, Winston AI oder ZeroGPT analysieren Texte auf statistische Muster, die KI-generierte Inhalte hinterlassen — Gleichförmigkeit im Satzbau, ungewöhnlich niedrige Perplexität, auffällige Wortwahlmuster.

Diese Tools sind ein zusätzliches Warnsignal, kein verlässliches Urteil. Ein menschlich klingender Prompt produziert KI-Text, den diese Detektoren nicht erkennen. Und umgekehrt können legitime, maschinell verfasste E-Mails (Buchungssysteme, Newslettertools) als „KI-generiert" markiert werden.

Sinnvoll einsetzbar: für einzelne verdächtige Mails, bei denen Inhalt und Kontext bereits Zweifel wecken. Als generellen Filter taugen diese Tools derzeit nicht.

Verhaltensbasierte Anomalieerkennung

Was moderne E-Mail-Security-Lösungen deutlich zuverlässiger leisten: sie analysieren Kommunikationsmuster. Microsoft Defender for Business und Google Workspace mit Enhanced Protection prüfen automatisch, ob ein Absender erstmalig schreibt, ob Uhrzeit und Sprache ungewöhnlich sind, ob die Mail Links zu Domains enthält, die erst kürzlich registriert wurden.

Diese verhaltensbasierte Analyse erkennt keine KI-generierte Sprache — aber sie erkennt, wenn etwas am Sendeverhalten nicht stimmt, das ein Mensch allein vielleicht übersieht.

Wann KI-Analyse hilfreich ist - und wann sie in die Irre führt

KI-generiert bedeutet nicht automatisch bösartig. Newsletter, Buchungsbestätigungen, automatisierte Statusmails — vieles davon ist maschinell erstellt und vollständig legitim. Ein KI-Erkennungshinweis ist ein Hinweis auf weitere Prüfung, kein Urteil über die Absicht des Absenders.

Umgekehrt gilt: Eine handgeschriebene, fehlerfreie Phishing-Mail ist genauso gefährlich wie eine KI-generierte. Die technische Verifikation des Absenders — Header, SPF/DKIM/DMARC — ist verlässlicher als jede Sprachanalyse.

Rechtlicher Rahmen in Österreich - DSGVO und TKG 2021

Wenn ein Angreifer Ihre Domain missbraucht und darüber Mails im Namen Ihres Unternehmens versendet, kann das für Sie rechtliche Konsequenzen haben — selbst wenn Sie Opfer sind. Empfänger könnten Schadensersatzansprüche prüfen, wenn sie durch gefälschte Mails mit Ihrem Firmennamen geschädigt wurden.

Relevanter für den Alltag ist die DSGVO-Meldepflicht: Wenn ein Mitarbeitender auf eine Phishing-Mail hereinfällt und dadurch Kundendaten kompromittiert werden, greift nach aktueller Rechtslage Artikel 33 DSGVO. Sie haben dann 72 Stunden Zeit, den Vorfall der österreichischen Datenschutzbehörde zu melden — unabhängig davon, ob Sie den Angriff verursacht haben oder Opfer waren.

Das TKG 2021 regelt in § 174 unerwünschte Nachrichten (Spam) und könnte in bestimmten Konstellationen relevant werden, wenn Ihre Domain für Massenversand missbraucht wird.

Empfehlung: Dokumentieren Sie, wie Ihr Unternehmen mit Phishing-Verdachtsfällen umgeht — wer intern informiert wird, wann externe Hilfe gerufen wird, wann eine behördliche Meldung erforderlich ist. Dieser Prozess muss kein langes Dokument sein, aber er muss existieren.

Hinweis: Dieser Artikel stellt keine Rechtsberatung dar. Für konkrete Fragen zu Meldepflichten und Haftung empfiehlt sich die Rücksprache mit einem Datenschutzbeauftragten oder Rechtsanwalt.

Wer KI-Tools im Unternehmen einsetzt und dabei Datenschutzfragen im Blick behalten möchte, findet in unserem Artikel zu KI DSGVO-konform einsetzen eine strukturierte Einordnung.

Tools im Überblick - kostenlos vs. kostenpflichtig für KMU-Budgets

TOOL	FUNKTION	KOSTEN	GEEIGNET FÜR
MXToolbox	SPF/DKIM/DMARC-Check	Kostenlos	Einmalige Prüfung
EasyDMARC	DMARC-Monitoring	Ab 0 €/Monat (Free Tier)	Kleine Teams
Microsoft Defender for Business	Integrierter E-Mail-Schutz	Ab ca. 3 €/User/Monat	M365-Nutzer
Google Workspace Enhanced Protection	Automatische Phishing-Erkennung	Im Workspace-Abo enthalten	Google-Nutzer
GPTZero / ZeroGPT	KI-Text-Erkennung	Kostenlos (limitiert)	Einzelne Mails prüfen
Proofpoint Essentials	Vollständige E-Mail-Security	Ab ca. 2–3 €/User/Monat	KMU mit dediziertem Budget

Für die meisten österreichischen KMU ist folgende Kombination ausreichend und realistisch: korrekte DNS-Einträge (SPF + DKIM + DMARC), ein gut konfiguriertes Microsoft 365 oder Google Workspace und regelmäßige Mitarbeiterschulung.

Der Kostenrahmen für ein 10-Personen-Unternehmen liegt damit realistisch bei 20–40 €/Monat — ohne zusätzliche Speziallösungen.

Der unterschätzte Faktor - Mitarbeitende als erste Verteidigungslinie

Selbst ein perfekt konfiguriertes DMARC schützt nicht vor Look-alike-Domains. Ein Angreifer, der `mein-buero.at` statt `meinbuero.at` registriert, besteht alle technischen Prüfungen problemlos. Die letzte Prüfinstanz ist der Mensch am Bildschirm.

Drei Verhaltensregeln, die jede:r sofort umsetzen kann

1. **Unerwartete Zahlungs- oder Zugangsdaten-Anfragen niemals per E-Mail bestätigen.** Rückfrage immer telefonisch, über eine Nummer die Sie selbst kennen — nicht die in der verdächtigen Mail.
2. **Links nicht anklicken, sondern die Domain manuell eintippen** oder ein gespeichertes Lesezeichen verwenden. Ein täuschend echter Link auf `erste-bank-sicherheit.at` führt nicht zur echten Erste Bank.
3. **Bei Unsicherheit den E-Mail-Header prüfen.** Die oben beschriebenen Schritte dauern zwei Minuten und liefern klare Ergebnisse.

Mini-Übung für das nächste Teammeeting (5 Minuten)

Zeigen Sie im Meeting zwei Absenderzeilen nebeneinander — eine echte, eine gefälschte mit manipuliertem Anzeigenamen. Lassen Sie das Team entscheiden und erklären Sie danach, wie die echte Absenderadresse sichtbar gemacht wird.

Aktuelle Beispiele aus Österreich — oft mit Screenshots echter Phishing-Mails — veröffentlicht Watchlist Internet laufend und kostenlos. Diese Website eignet sich gut als Ausgangsmaterial für solche Übungen.

Schritt-für-Schritt: So verifizieren Sie einen verdächtigen Absender heute noch

1. Anzeigename ignorieren Echte Absenderadresse im E-Mail-Client einblenden — in Outlook über den Klick auf den Absendernamen, in Gmail über den Pfeil im Kopfbereich.

2. Domain prüfen Stimmt die Domain mit der offiziellen Website überein? Für österreichische .at-Domains: WHOIS-Abfrage bei `nic.at`. Für andere Domains: `whois.domaintools.com`.

3. E-Mail-Header analysieren Header öffnen (Anleitung oben), das Feld „Authentication-Results“ suchen. Steht dort `spf=pass`, `dkim=pass`, `dmarc=pass`? Bei `fail` bei einem oder mehreren Einträgen: erhöhte Vorsicht.

4. MXToolbox Quick Check Die Domain des Absenders in MXToolbox eingeben und SPF- sowie DMARC-Konfiguration prüfen. Fehlt ein DMARC-Eintrag, deutet das auf eine schlecht gesicherte Domain hin.

5. Im Zweifel: Rückfrage über bekannten Kanal Nicht per „Antworten" auf die verdächtige Mail, sondern über Telefon oder die Kontaktadresse von der offiziellen Website.

6. Verdachtsfall dokumentieren Screenshot der Mail, Absenderadresse notieren, internen Meldeweg durchlaufen. Bei konkretem Schadenseintritt: Datenschutzbeauftragten oder Rechtsanwalt kontaktieren.

Praxis-Tipp: Was ein KMU-Setup ohne IT-Abteilung leisten kann

Ein konkretes Szenario: Ein Buchhaltungsbüro in Wien, 8 Mitarbeitende, Microsoft 365 Business Basic. Was ist hier mit Bordmitteln möglich?

Checkliste für das Basis-Setup: - SPF-Eintrag prüfen und bei Bedarf setzen lassen (Hosting-Provider, ca. 15 Minuten) - DKIM aktivieren (M365 Admin Center → Exchange → E-Mail-Authentifizierung, geführte Einrichtung) - DMARC-Eintrag als TXT-Eintrag im DNS ergänzen (Vorlage liefert Microsoft in der eigenen Dokumentation) - Enhanced Phishing Protection in Windows 11 aktivieren (Einstellungen → Datenschutz & Sicherheit → Windows-Sicherheit → App- & Browsersteuerung)

Dieser Aufwand ist kein Vollzeitprojekt. Mit einem einmaligen Setup von 2–3 Stunden — oder mit externer Unterstützung in derselben Zeit — steht die technische Grundlage. Danach läuft die Konfiguration im Hintergrund.

Wenn Sie nicht sicher sind, ob Ihr aktuelles E-Mail-Setup diese Grundkonfiguration bereits erfüllt, oder wenn Sie eine strukturierte Einschätzung Ihrer gesamten IT-Security-Basis möchten: Im kostenlosen Beratungsgespräch klären wir gemeinsam, wo Ihr Unternehmen steht und welche Schritte wirklich Priorität haben.

Nächste Schritte

Die drei wichtigsten Sofortmaßnahmen, die Sie noch diese Woche angehen können:

1. **SPF, DKIM und DMARC prüfen** — MXToolbox und EasyDMARC sind kostenlos, die Prüfung dauert wenige Minuten.
2. **Mitarbeitende sensibilisieren** — die 5-Minuten-Übung aus dem Teammeeting-Abschnitt oben ist ein konkreter Einstieg, kein aufwendiges Schulungsprogramm.
3. **Verdachtsfall-Prozess definieren** — ein einfaches Dokument: wer intern informiert wird, wann externe Hilfe gerufen wird, wann eine behördliche Meldung nötig ist.

Wenn Sie sich nicht sicher sind, ob Ihre E-Mail-Konfiguration diese Schutzebenen bereits umfasst — oder wenn Sie das Thema KI-Sicherheit in Ihrem Unternehmen grundsätzlicher angehen möchten: Vereinbaren Sie ein unverbindliches 30-Minuten-Beratungsgespräch mit dem Strukturaflow IT-Team. Wir schauen uns gemeinsam an, wo die größten Lücken sind und was für Ihr Team realistisch umsetzbar ist — ohne technisches Vorwissen Ihrerseits.

Die meisten KMU in Österreich können ihren E-Mail-Schutz mit überschaubarem Aufwand deutlich verbessern. Der erste Schritt ist der schwierigste — und der dauert oft weniger als eine Stunde.