JUSTIN BOCH SOLUTIONS EST. 2025

PRESSEMITTEILUNG

Jede zweite Firmen-E-Mail in NRW lässt sich fälschen, ohne dass es auffällt

Eine Untersuchung von 15.452 Unternehmen in Nordrhein-Westfalen zeigt: Bei 54 Prozent kann ein Fremder eine E-Mail im Namen des Unternehmens verschicken, ohne dass der empfangende Mailserver sie zuverlässig abweisen würde. Das Handwerk liegt dabei im Mittelfeld — schlechter stehen Arztpraxen und Schulen da.

Münster, 22. Oktober 2026 — Wer im Namen eines Unternehmens aus Nordrhein-Westfalen eine E-Mail verschicken will, muss dafür kein Passwort knacken. Bei der Mehrheit genügt es, den Absender hinzuschreiben. Das ist das Ergebnis einer Untersuchung, die das Münsteraner IT-Unternehmen Justin Boch - Solutions im Oktober 2026 durchgeführt hat.

Geprüft wurden die öffentlich abrufbaren E-Mail-Einstellungen von 15.452 Unternehmen und Einrichtungen aus 14 Branchen — darunter 4.838 Handwerksbetriebe, 2.533 Schulen, 2.274 Arztpraxen und 1.673 Apotheken. Bei 14.132 war ein Mailbetrieb erkennbar; nur sie gingen in die Auswertung ein.

> **Über alle Branchen: 54,3 Prozent haben eine kritische Lücke. Vollständig abgesichert sind 4,6 Prozent.**

Das Handwerk liegt im Mittelfeld

Die naheliegende Vermutung — Handwerksbetriebe hinken bei der Digitalisierung hinterher — bestätigt sich nicht. Von 14 geprüften Branchen liegt das Handwerk auf Platz sieben.

Branche	geprüft	kritische Lücke
Banken und Sparkassen	209	**16,3 %**
IT-Dienstleister	611	31,9 %
Werbe- und Webagenturen	232	44,0 %
Apotheken	1.515	45,1 %
Versicherungsbüros	258	48,1 %
Immobilienmakler	359	52,4 %
Handwerksbetriebe	**4.410**	**55,7 %**
Rechtsanwälte	625	56,0 %
Kfz-Werkstätten	955	57,4 %
Architekturbüros	173	58,4 %
Steuerberater	360	58,9 %
Arztpraxen	2.125	60,2 %
Schulen	2.269	60,6 %
Handwerksorganisationen	23	60,9 %

Berufsgruppen, deren Geschäft aus Formvorschriften und Schriftverkehr besteht, stehen nicht besser da: Bei Steuerberatern und Rechtsanwälten ist der Anteil kritischer Lücken höher als im Handwerk.

Zwei Branchen zeigen, dass es geht

Banken und Sparkassen fallen deutlich aus dem Rahmen: Nur 16,3 Prozent haben eine kritische Lücke. Bei den IT-Dienstleistern sind es 31,9 Prozent, und sie stellen mit 20,1 Prozent den höchsten Anteil vollständig abgesicherter Unternehmen.

Das ist der wichtigste Befund der Untersuchung: Die nötigen Einträge sind kostenlos, seit Jahren standardisiert und in zwei Branchen bereits verbreitet. Es handelt sich nicht um ein technisches, sondern um ein Umsetzungsproblem.

Eingerichtet und nie eingeschaltet

Der auffälligste Einzelbefund betrifft Unternehmen, die bereits gehandelt haben. **1.421 Handwerksbetriebe (32,2 Prozent)** haben eine Abwehrregel hinterlegt, sie aber auf der Stufe „nur beobachten" belassen. Gefälschte Nachrichten werden dort erkannt — und trotzdem zugestellt.

Diese Betriebe sind schlechter gestellt als jene ohne jeden Schutz, weil sie sich für geschützt halten. Am häufigsten tritt das Muster bei Werbe- und Webagenturen auf: Dort haben **37,5 Prozent** den Schutz eingerichtet und nicht scharf gestellt — der höchste Wert aller 14 Branchen.

Weitere Befunde im Handwerk

Von den 4.410 Handwerksbetrieben mit erkennbarem Mailbetrieb:

- **1.902 (43,1 %)** haben keine Regel hinterlegt, was mit gefälschten Nachrichten in ihrem Namen geschehen soll.
- **795 (18,0 %)** haben nicht veröffentlicht, wer in ihrem Namen Mails verschicken darf.
- **883 (20,0 %)** nutzen Microsoft 365, wo die nötigen Einstellungen vorhanden, aber nicht aktiviert sind.
- Bei **3.562 (80,8 %)** ließ sich unter elf verbreiteten Kennungen keine digitale Signatur finden. Diese Zahl ist eine Obergrenze — siehe Methodik.

Das Münsterland schneidet am schlechtesten ab

Von den fünf Regierungsbezirken liegt Münster beim Handwerk auf dem letzten Platz: **61,3 Prozent** kritische Lücken gegenüber 55,7 Prozent im Landesdurchschnitt.

Regierungsbezirk	Betriebe	kritische Lücke
Düsseldorf	797	52,7 %
Köln	1.380	53,4 %
Detmold	716	56,8 %
Arnsberg	912	57,3 %
Münster	**605**	**61,3 %**

Nach Gewerken stehen Maler und Zimmerer am schlechtesten da: bei beiden haben rund 62 Prozent eine kritische Lücke.

Auch die Organisationen des Handwerks sind betroffen

Von 23 Handwerkskammern, Kreishandwerkerschaften und Innungen in Nordrhein-Westfalen, die sich prüfen ließen, haben **14 eine kritische Lücke**. Vollständig abgesichert sind zwei: die Handwerkskammer Münster und die Kreishandwerkerschaft Coesfeld.

Diese Teilgruppe ist mit 23 Fällen klein, und die Namen der betroffenen Organisationen werden hier nicht genannt. Die Größenordnung ist dennoch bemerkenswert, weil diese Einrichtungen ihre Mitglieder zur Digitalisierung beraten.

Was das praktisch bedeutet

Der Schaden entsteht meist nicht im Unternehmen, sondern beim Kunden. Üblich ist die gefälschte Rechnung: Sie trägt den Namen des Betriebs, bezieht sich auf einen echten Auftrag und nennt eine fremde Bankverbindung. Weder der Kunde noch sein E-Mail-Programm können den Unterschied erkennen, solange das Unternehmen die nötigen Einträge nicht veröffentlicht hat.

„Die meisten Betriebe haben in den letzten Jahren viel für ihre IT getan — neue Rechner, Cloud, digitale Zeiterfassung", sagt Justin Boch, Inhaber von Justin Boch - Solutions in Münster. „Die E-Mail ist dabei so geblieben, wie sie vor zehn Jahren eingerichtet wurde."

„Am schlechtesten stehen die Betriebe da, die angefangen und nicht beendet haben", sagt Boch. „Der Schutz ist eingerichtet, er läuft auf Beobachten, und niemand hat ihn je scharf gestellt. Die halten sich für geschützt und sind es nicht."

Was Unternehmen tun können

Die nötigen Einträge heißen SPF, DKIM und DMARC. Sie werden einmal beim Domain-Anbieter hinterlegt und kosten im laufenden Betrieb nichts. Drei Schritte:

1. **Prüfen lassen**, ob alle drei Einträge vorhanden sind — der IT-Dienstleister oder Webbetreuer kann das in wenigen Minuten beantworten.
2. **Fehlende Einträge ergänzen.** Bei Microsoft 365 und Google Workspace ist die Funktion enthalten und muss nur aktiviert werden.
3. **DMARC scharf stellen.** Bleibt die Regel auf „nur beobachten" stehen, werden gefälschte Mails weiterhin zugestellt. Üblich ist ein Übergang von vier Wochen Beobachtung auf Abweisen.

Einen kostenlosen Selbsttest stellt Justin Boch - Solutions unter **boch-solutions.de/email-check** bereit. Dort wird dieselbe Prüfung für die eigene Domain ausgeführt und das Ergebnis als Bericht zugeschickt.

Die vollständigen Ergebnisse aller 14 Branchen, die regionale Verteilung und die Methodik sind unter **boch-solutions.de/studie/email-sicherheit-nrw-2026** abrufbar.

Zur Methodik

Grundgesamtheit. Ausgewertet wurden alle Unternehmen und Einrichtungen in Nordrhein-Westfalen, die in OpenStreetMap in einer der 14 geprüften Kategorien erfasst sind und dort eine Website hinterlegt haben — 15.452 eindeutige Domains. Erhebung am 14. und 15. Oktober 2026. Datenquelle: OpenStreetMap-Mitwirkende, verfügbar unter der Open Database License (ODbL).

Erhebung. Gelesen wurden ausschließlich öffentliche Einträge im Domain Name System (SPF, DKIM, DMARC, MX) — dieselben Angaben, die jeder Mailserver weltweit abfragt, bevor er eine Nachricht annimmt. Es wurde kein System angegriffen, keine Mail verschickt und kein Zugang verwendet. Einzelne Unternehmen werden nicht namentlich genannt.

Was „kritische Lücke" bedeutet. Ein Unternehmen gilt als kritisch, wenn SPF oder DMARC fehlen, widersprüchlich sind oder eine begonnene Einrichtung nachweislich unvollständig blieb. Beide Angaben stehen im DNS an festen, eindeutigen Stellen und sind von außen zweifelsfrei feststellbar.

Einschränkungen, die wir ausdrücklich benennen:

1. **Digitale Signaturen lassen sich von außen nicht sicher nachweisen.** DKIM-Schlüssel liegen unter frei wählbaren Kennungen; diese Untersuchung fragt elf verbreitete ab. Wer eine eigene Kennung nutzt, wird als „nicht gefunden" gezählt, obwohl er signiert. Der Wert von 80,8 Prozent ist deshalb eine Obergrenze, und der Anteil vollständig abgesicherter Unternehmen entsprechend eine

Untergrenze. Die Einstufung „kritische Lücke" ist davon nicht betroffen, weil sie auf SPF und DMARC beruht.

2. **Die Auswahl ist nicht repräsentativ.** Erfasst sind nur Unternehmen, die in OpenStreetMap stehen und eine Website betreiben. Sie sind tendenziell digital weiter aufgestellt als der Durchschnitt — das tatsächliche Bild dürfte eher schlechter ausfallen. Die Zahlen gelten für die untersuchte Gruppe, nicht für „die Unternehmen in NRW" insgesamt.
3. **Kleine Teilgruppen.** Handwerksorganisationen (23), Architekturbüros (173) und Banken (209) erlauben keine belastbaren Quoten, sondern zeigen Größenordnungen.
4. **Ausschlüsse.** 1.320 der 15.452 Domains zeigten keinen erkennbaren Mailbetrieb und wurden nicht ausgewertet.

Nachvollziehbarkeit. Die Prüfung lässt sich jederzeit wiederholen; die Methode ist im kostenlosen Selbsttest unter boch-solutions.de/email-check öffentlich nachvollziehbar. Alle Zahlen dieser Mitteilung stehen samt Methodik und Einschränkungen unter boch-solutions.de/studie/email-sicherheit-nrw-2026. Die Ergebnisse je Unternehmen liegen vor und können Redaktionen in anonymisierter Form zur Prüfung zur Verfügung gestellt werden.

Über Justin Boch - Solutions

Justin Boch - Solutions ist ein IT-Dienstleister aus Münster mit Schwerpunkt auf Handwerksbetrieben in Münster und im Münsterland. Das Leistungsspektrum umfasst Einrichtung und Betreuung von Microsoft 365, die Absicherung von Firmen-E-Mail sowie Konzeption und Entwicklung von Unternehmenswebseiten. Das Unternehmen besteht seit 2025.

Pressekontakt

Justin Boch, Justin Boch - Solutions, Münster. Telefon 0251 28069471, kontakt@boch-solutions.de, boch-solutions.de

---