Drohmails mit eigener E-Mail-Adresse: Ursachen, Folgen und Schutz

26.08.2026, 15:21 | IT, New Media & Software

Pressemitteilung von: *prtesse*

Domain Spoofing (KI-generiertes Symbolbild)

Wenn plötzlich mehrere Drohmails von der eigenen E-Mail-Adresse eintreffen, ist die Verunsicherung groß. Wurde das eigene Konto gehackt? Wurden persönliche Daten gestohlen? Oder steckt etwas anderes dahinter?

In vielen Fällen handelt es sich nicht um einen direkten Kontohack, sondern um sogenanntes **E-Mail-Spoofing**. Dabei verwenden Kriminelle die eigene E-Mail-Adresse oder Domain lediglich als sichtbaren Absender, während die Nachrichten tatsächlich von fremden Systemen verschickt werden.

Gerade wenn innerhalb kurzer Zeit zahlreiche nahezu identische Droh- oder Erpressungsmails eintreffen, spricht vieles für eine automatisierte Spam- oder Erpressungswelle.

Woran lässt sich ein Spoofing-Angriff erkennen?

Typische Anzeichen sind:

- Mehrere baugleiche oder sehr ähnliche Drohmails treffen innerhalb kurzer Zeit ein.
- Andere Personen berichten, ebenfalls Nachrichten von der eigenen Adresse erhalten zu haben.
- Es häufen sich Bounce- oder Zustellfehler für E-Mails, die man selbst nie verschickt hat.
- Im E-Mail-Konto sind keine verdächtigen Anmeldungen oder unbekannten Geräte erkennbar.
- Im Ordner „Gesendet“ befinden sich keine unbekannten Nachrichten.
- Es wurden keine unbekannten Weiterleitungen oder Filterregeln eingerichtet.

Treffen mehrere dieser Merkmale zu, ist ein tatsächlicher Kontohack nicht zwingend die Ursache.

Was Betroffene jetzt tun sollten

Zunächst gilt: **Ruhe bewahren.** Eine Drohmail mit der eigenen Adresse als Absender ist noch kein Beweis dafür, dass

das E-Mail-Konto kompromittiert wurde.

Betroffene sollten insbesondere:

- **Nicht auf die Forderungen eingehen oder Zahlungen leisten.** Gerade bei Bitcoin-Zahlungen besteht in der Regel keine Möglichkeit, das Geld zurückzuholen.
- **Nicht auf Links oder Anhänge in den Nachrichten klicken.** Diese können zu Phishing-Seiten oder Schadsoftware führen.
- **Nicht auf die Drohmails antworten.** Eine Reaktion kann bestätigen, dass die Adresse aktiv genutzt wird.
- **Das eigene E-Mail-Konto überprüfen.** Dazu gehören Login-Aktivitäten, gesendete Nachrichten, Weiterleitungen, Filter und andere Kontoeinstellungen.
- **Das Passwort vorsorglich ändern**, insbesondere wenn Hinweise auf eine tatsächliche Kompromittierung bestehen.
- **Die Zwei-Faktor-Authentifizierung aktivieren**, sofern der verwendete E-Mail-Dienst dies unterstützt.
- **Die eigene Domain und deren E-Mail-Konfiguration überprüfen lassen.**

Was passiert beim E-Mail-Spoofing?

Beim Spoofing wird die Absenderadresse einer E-Mail manipuliert. Kriminelle können dadurch beispielsweise eine Adresse aus dem eigenen Unternehmen oder sogar die eigene Adresse als sichtbaren Absender einsetzen, ohne tatsächlich Zugriff auf das betreffende Postfach zu besitzen.

Bei größeren Kampagnen geschieht der Versand automatisiert. Dabei können innerhalb kurzer Zeit sehr viele Nachrichten mit gefälschten Absenderadressen verschickt werden.

Das bedeutet: **Dass eine Drohmail scheinbar vom eigenen Konto stammt, bedeutet nicht automatisch, dass jemand Zugriff auf das Konto hat.**

Entscheidend ist deshalb die Unterscheidung zwischen einem kompromittierten E-Mail-Konto und dem Missbrauch der eigenen Domain als Absender.

Domain-Spoofing oder echter Konto-Hack?

Einige Merkmale können bei der ersten Einschätzung helfen:

MerkmalDomain-SpoofingEchter Konto-HackUnbekannte Mails im PostausgangEher neinHäufig jaKonto normal erreichbarJaUnter Umständen neinUnbekannte Login-AktivitätenMeist neinMöglichUnbekannte WeiterleitungsregelnMeist neinMöglichEigene Adresse als Absender missbrauchtJaMöglichErste MaßnahmeE-Mail-Domain analysierenZugang sofort absichern

Diese Übersicht ersetzt keine technische Untersuchung. Insbesondere bei verdächtigen Login-Aktivitäten, unbekannten Regeln oder Nachrichten im Postausgang sollte von einer möglichen Kontokompromittierung ausgegangen werden.

Warum eine Domain-Analyse sinnvoll ist

Ein einzelner Spoofing-Versuch lässt sich nicht immer verhindern. Unternehmen können jedoch ihre Domain so konfigurieren, dass empfangende Mailserver besser erkennen können, welche Nachrichten tatsächlich von autorisierten Mailservern stammen.

Dabei spielen unter anderem **SPF, DKIM und DMARC** eine wichtige Rolle. Eine korrekt konfigurierte E-Mail-Authentifizierung kann dazu beitragen, den Missbrauch einer Domain als gefälschten Absender einzuschränken.

Gleichzeitig sollte die E-Mail-Reputation der Domain im Blick behalten werden. Wiederholter Missbrauch als Absender

kann dazu führen, dass legitime Nachrichten schwieriger zugestellt werden oder häufiger in Spam-Ordnern landen.

Drohmails nicht unterschätzen – aber richtig einordnen

Mehrere Drohmails innerhalb kurzer Zeit wirken zunächst wie ein gezielter Angriff. Häufig sind solche Nachrichten jedoch Bestandteil automatisierter Massenkampagnen.

Das Wichtigste ist daher eine strukturierte Prüfung: **Wurde tatsächlich auf das Konto zugegriffen oder wird lediglich die eigene E-Mail-Adresse beziehungsweise Domain als Absender gefälscht?**

Wer unsicher ist, sollte die Situation technisch analysieren lassen, statt auf die Forderungen der Absender einzugehen.

Kostenlose Analyse anfragen

Betroffene können ihre Situation kostenlos prüfen lassen und erfahren, welche Schritte zur Absicherung der eigenen E-Mail-Kommunikation sinnvoll sind.

Jetzt kostenlose Analyse anfragen und die eigene Domain überprüfen lassen.

PROTECTA360©

Mayrmeuhlweg 3
5303 thalgau
Österreich

Portrait

PROTECTA360 IT & Cyber Security Unternehmen

News-ID: 1321679 • Views: 53 (Stand: 28.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1321679/Drohmails-mit-eigener-E-Mail-Adresse-Ursachen-Folgen-und-Schutz.html