

Wesentliche Protokolle

HTTP(S), FTP(S), DHCP, SMTP, POP4, IMAP4 und Spoofing mit Telnet

Tom Gries | Berlin | Oktober 2023



Dokumenten URL:

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

Autor:

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

Lizenz:

Creative Commons BY-NC-ND

Version:

7.0.0 vom 20.10.2023





HTTP(S)

Jeder Webserver "spricht" **HTTP**. In den letzten Jahren auch immer mehr die verschlüsselte Variante **HTTPS**.

HTTP ist ein Klartextprotokoll. Wenn man den Aufbau kennt, kann man mit Telnet "httpisch sprechen".

```
Kali - LiveHacking
root@TOMO-DesktopPC:~# telnet example.net http
Trying 93.184.216.34...
Connected to example.net.
Escape character is '^]'.
GET / HTTP/1.0
HOST: example.net
```



FTP(S)/(S)FTP

FTP ist eins der ältesten Protokolle und Anwendungen. In den Anfangszeiten des Internets wurden so Daten ausgetauscht (HTTP gab es da noch nicht).

FTP wird in aktiv und passiv unterschieden.

```
Kali - LiveHacking
root@TOMO-DesktopPC:~# ncftp ftp.uni-kl.de
NcFTP 3.2.5 (Feb 02, 2011) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 131.246.123.4...
(vsFTPD 2.3.2)
Logging in...
*****
***      Welcome to the Anonymous FTP Server at the      ***
***                        University of Kaiserslautern      ***
*****

If you have any problems, ideas or whatever, please feel
free to write an Electronic Mail to

ftpadm@uni-kl.de

*****
ALL TRANSFERS WILL BE LOGGED
*****
Login successful.
Logged in to ftp.uni-kl.de.
ncftp / > bye
```



DHCP steht für „Dynamic Host Configuration Protocol“. Es ermöglicht die Zuweisung der Netzwerkkonfiguration, wie zum Beispiel

- IP Adresse (IPv4 und/oder IPv6)

- Subnetmask

- Default Gateway

- Nameserver (DNS – Primary und/oder Secondary)

- NTP-Server

- Hostname

an Clients durch einen Server für eine bestimmte Zeit (Lease Time).



SMTP - MX ermitteln mit dig

SMTP gehört zu den Mail Protokollen und ist für das Versenden und Weiterleiten von Emails zwischen den beteiligten Systemen (MUA und MTA) zuständig.

```
Kali - LiveHacking
root@TOM0-DesktopPC:~# dig t-systems.com MX

; <<>> DiG 9.16.6-Debian <<>> t-systems.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21274
;; flags: qr rd ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;t-systems.com.                IN      MX

;; ANSWER SECTION:
t-systems.com.                0      IN      MX      100 mailin12.telekom.de.
t-systems.com.                0      IN      MX      100 mailin32.telekom.de.
t-systems.com.                0      IN      MX      100 mailin22.telekom.de.
t-systems.com.                0      IN      MX      100 mailin42.telekom.de.

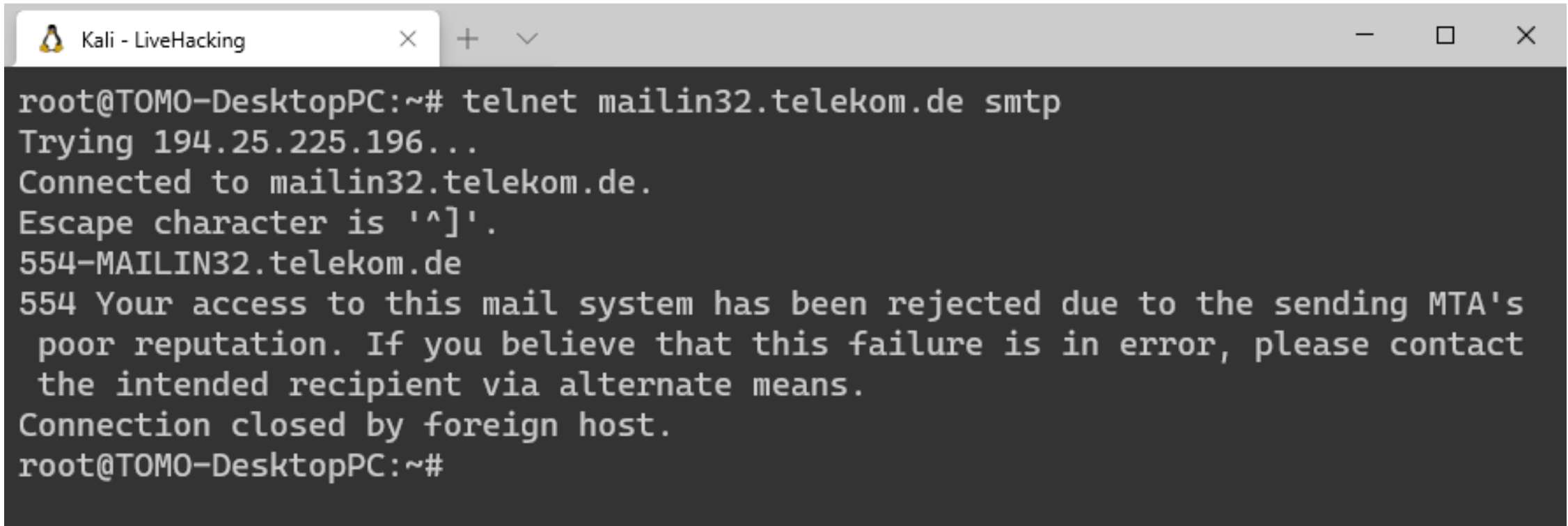
;; Query time: 20 msec
;; SERVER: 172.24.80.1#53(172.24.80.1)
;; WHEN: Tue Jan 19 14:33:01 CET 2021
;; MSG SIZE rcvd: 184

root@TOM0-DesktopPC:~#
```



SMTP - Mailversand mit Telnet

Der Versand einer Email vom Präsentationsrechner im Homeoffice funktioniert nicht. Der Telekom Mailserver erkennt, dass es sich um eine dynamisch zugewiesene IP Adresse eines ISP handelt und verweigert daher den Verbindungsaufbau.



```
Kali - LiveHacking
root@TOMO-DesktopPC:~# telnet mailin32.telekom.de smtp
Trying 194.25.225.196...
Connected to mailin32.telekom.de.
Escape character is '^]'.
554-MAILIN32.telekom.de
554 Your access to this mail system has been rejected due to the sending MTA's
  poor reputation. If you believe that this failure is in error, please contact
  the intended recipient via alternate means.
Connection closed by foreign host.
root@TOMO-DesktopPC:~#
```



Mailversand mit Telnet - "MAIL FROM" und "From" unterschiedlich

Von einem Rechner aus dem Internet funktioniert es, da dieser eine fest zugewiesene IP Adresse hat.

Demo 1:

Die Emailadressen des tatsächlichen und angezeigten Empfänger sind nicht identisch.

```
tomo@penttesttux:~$ telnet mailin32.telekom.de smtp
Trying 194.25.225.196...
Connected to mailin32.telekom.de.
Escape character is '^]'.
220 MAILIN32.telekom.de ESMTP
MAIL FROM: <LiveHacking@outlook.de>
RCPT TO: <Tom.Gries@t-systems.com>
DATA
From: "Schink, Michael" <Michael.Schink@telekom.de>
To: "Gries, Tom" <Tom.Gries@t-systems.com>
Reply-to: "Schink, Michael" <LiveHacking@outlook.de>
Subject: Telnet Demo

Hallo Tom,

dies ist eine Telnet Demo vom Workshop.

LiveHacking
.
250 sender <LiveHacking@outlook.de> ok
250 recipient <Tom.Gries@t-systems.com> ok
354 go ahead
250 ok: Message 431836274 accepted
QUIT
221 MAILIN32.telekom.de
Connection closed by foreign host.
tomo@penttesttux:~$
```

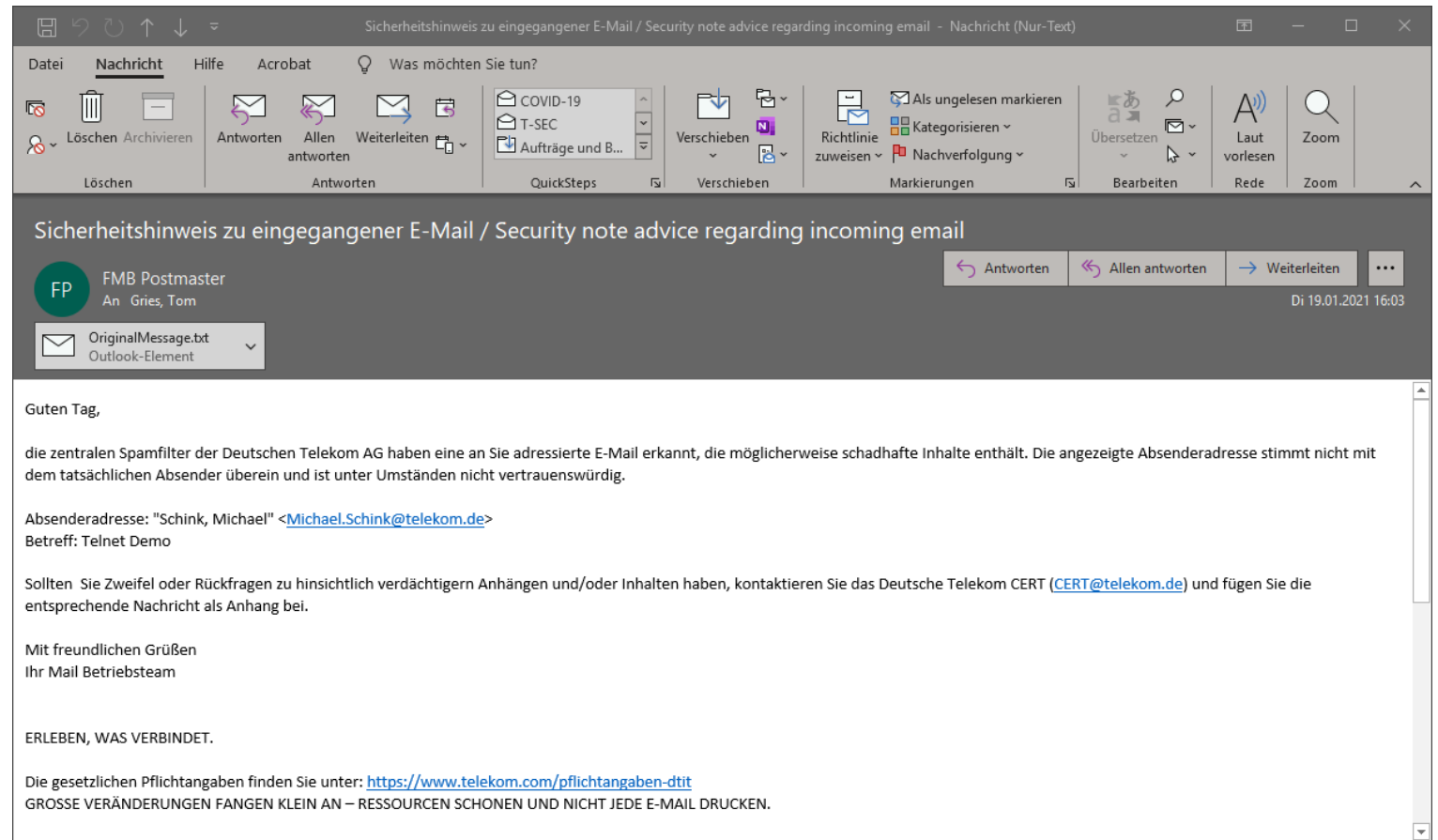


Mailversand mit Telnet - "MAIL FROM" und "From" unterschiedlich

Noch Demo 1:

Der Spamfilter erkennt, dass hier etwas nicht stimmt und warnt den Empfänger.

Das ist nicht bei allen Mail-Gateways so. Viele nehmen solche Emails ohne weitere Hinweise an den Empfänger an.

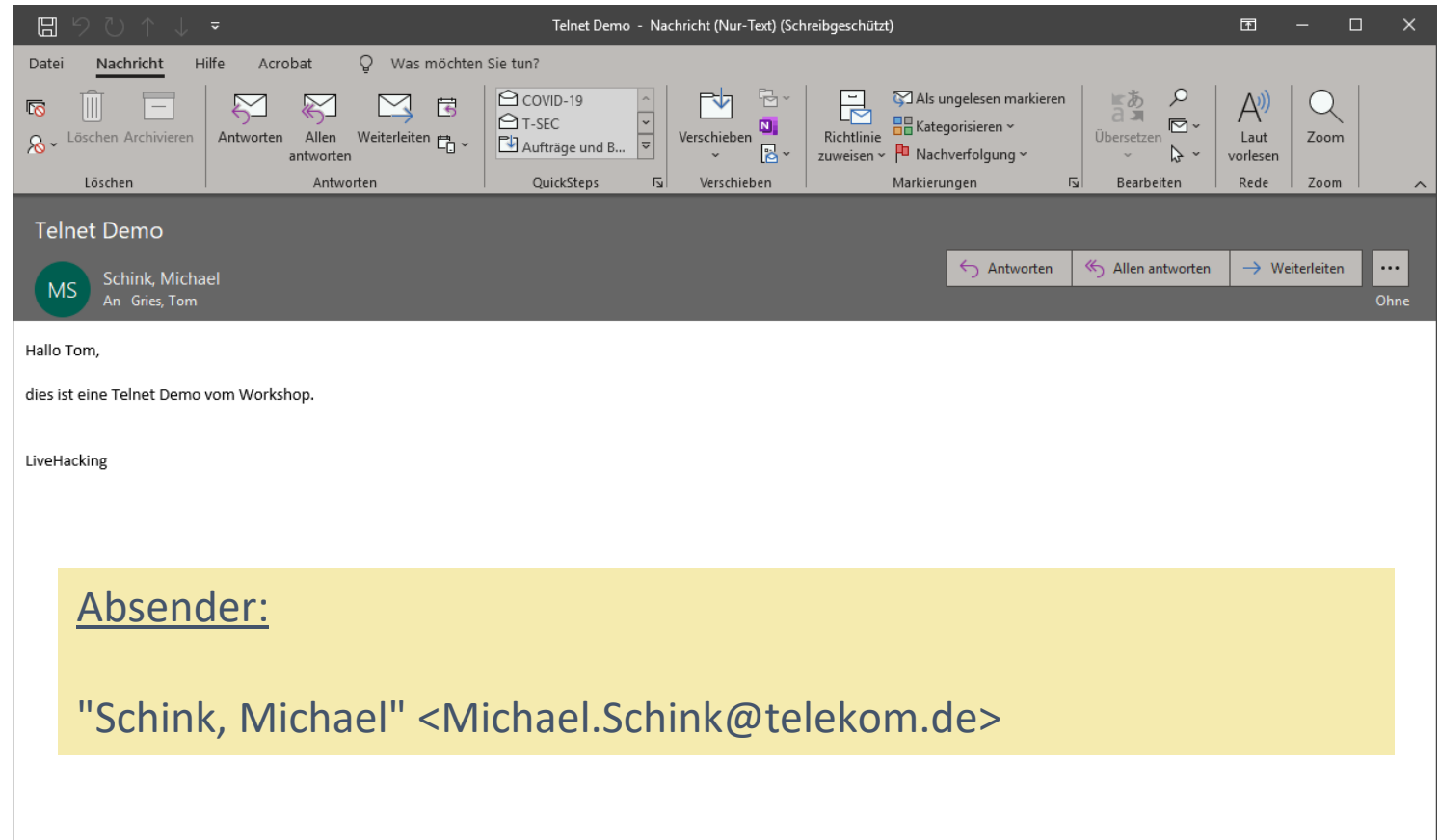




Mailversand mit Telnet - "MAIL FROM" und "From" unterschiedlich

Noch Demo 1:

Die eingebettete Mail sieht ganz normal aus. Der Absender ist in dieser Demo augenscheinlich ein interner Kollege.

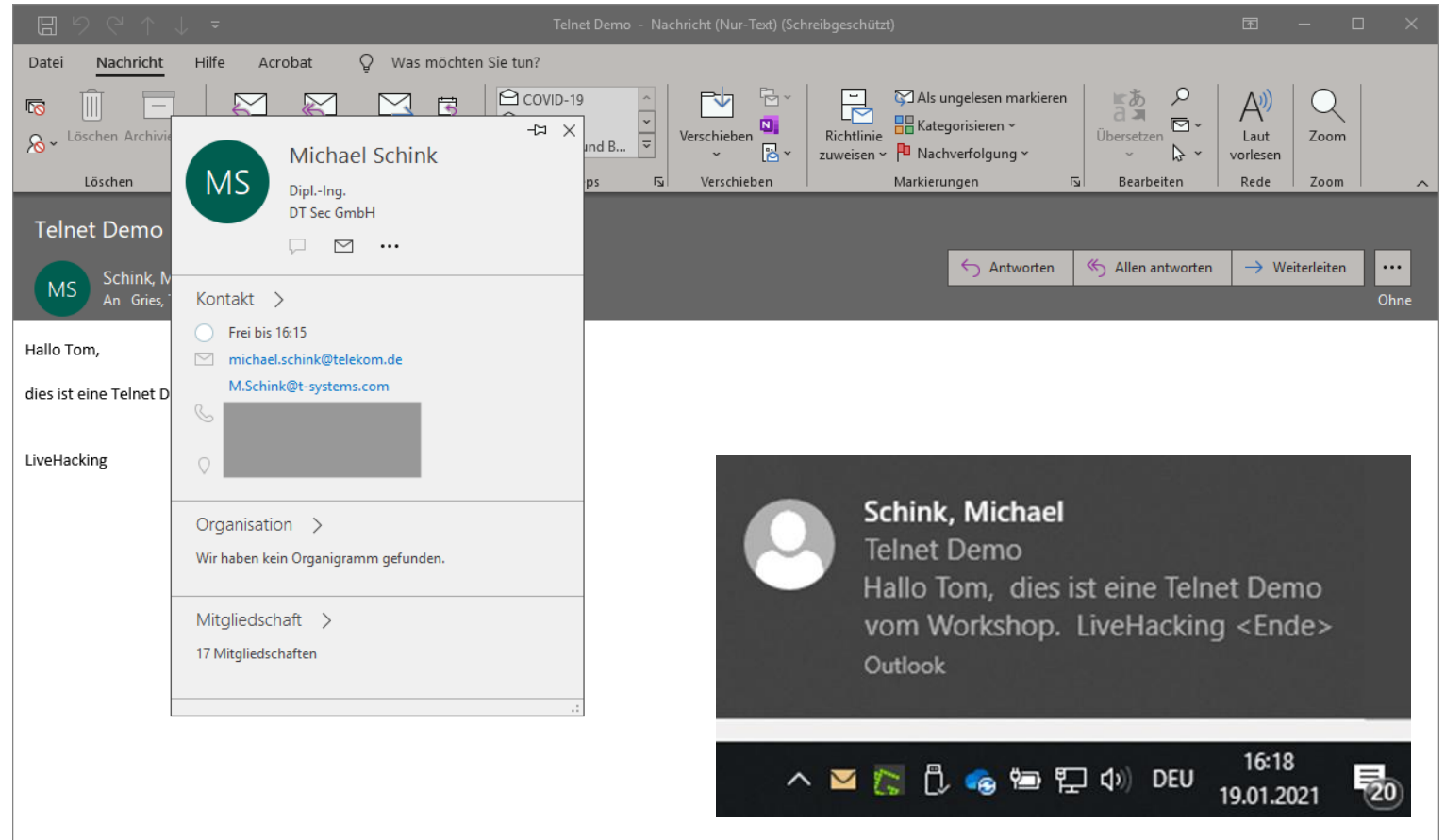




Mailversand mit Telnet - "MAIL FROM" und "From" unterschiedlich

Noch Demo 1:

Bei einem Klick auf den Namen des vermeintlichen Absenders sieht es auch so aus, als wenn die Mail von intern kommt: Es werden die Informationen aus dem Adressbuch angezeigt. Und auch das Pop-Up aus dem Infobereich sieht ganz normal aus.

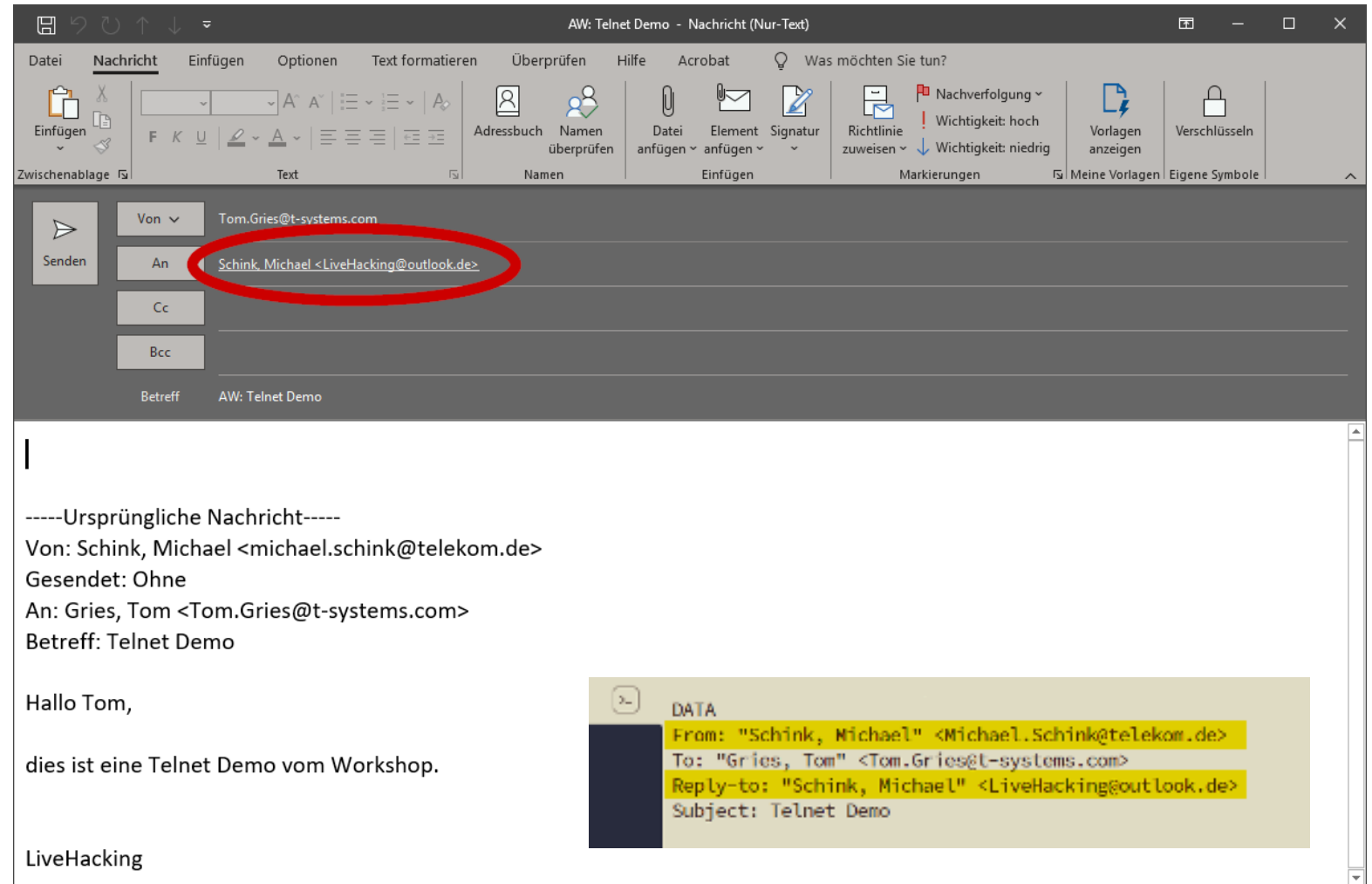




Mailversand mit Telnet - "MAIL FROM" und "From" unterschiedlich

Noch Demo 1:

Wenn man antworten möchte, sieht man beim genauen Hinschauen aber, dass eine falsche Email-adresse für den vermeintlichen internen Kollegen verwendet wurde.



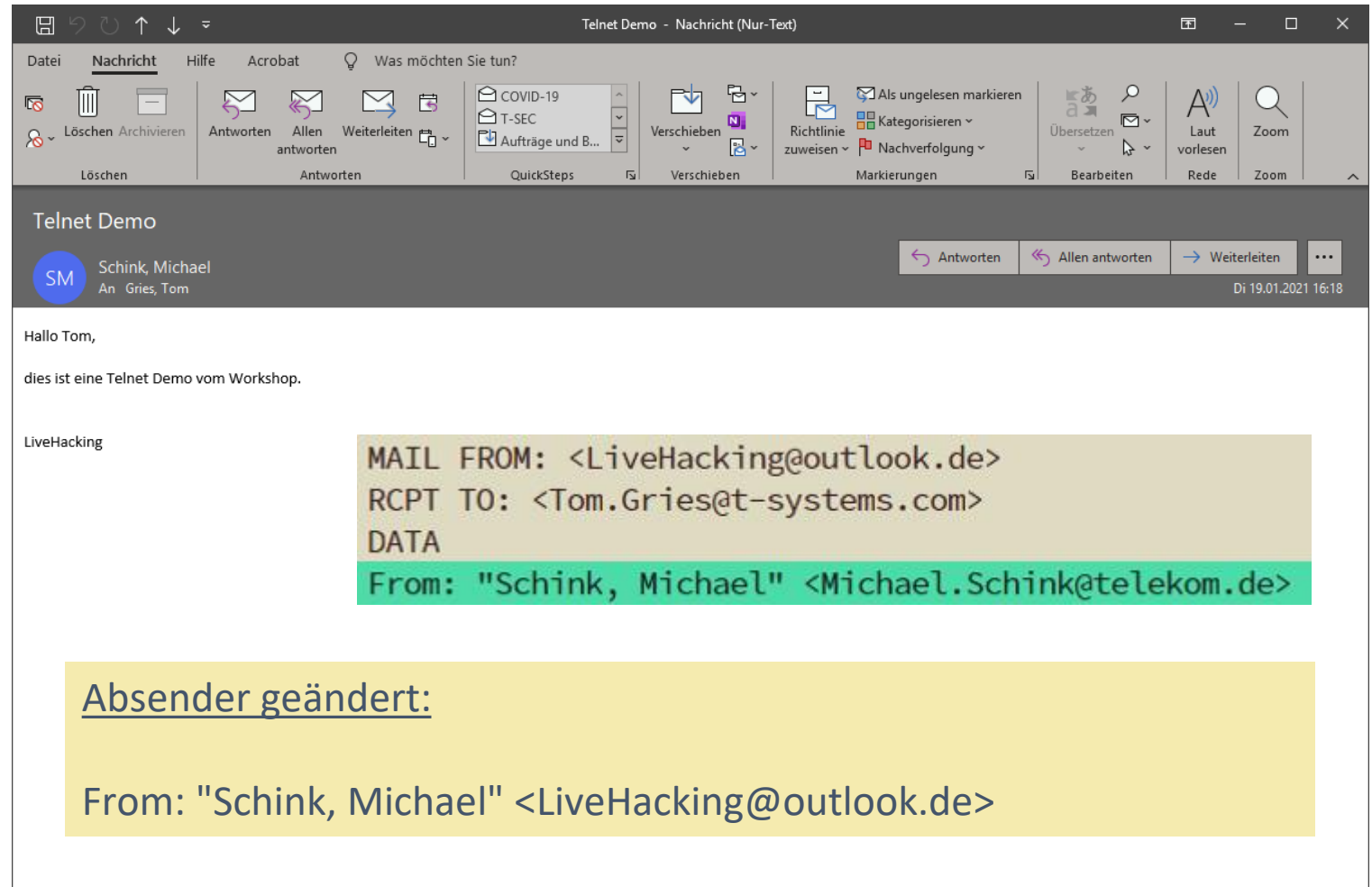


Mailversand mit Telnet - "MAIL FROM" und "From" identisch

Demo 2:

Diesmal gibt es keinen Hinweis vom Spamfilter, denn hier stimmen der angezeigte und der tatsächliche Absender überein.

Outlook unterdrückt die Emailadresse vom Absender, so dass man die Fälschung nicht sofort erkennt.



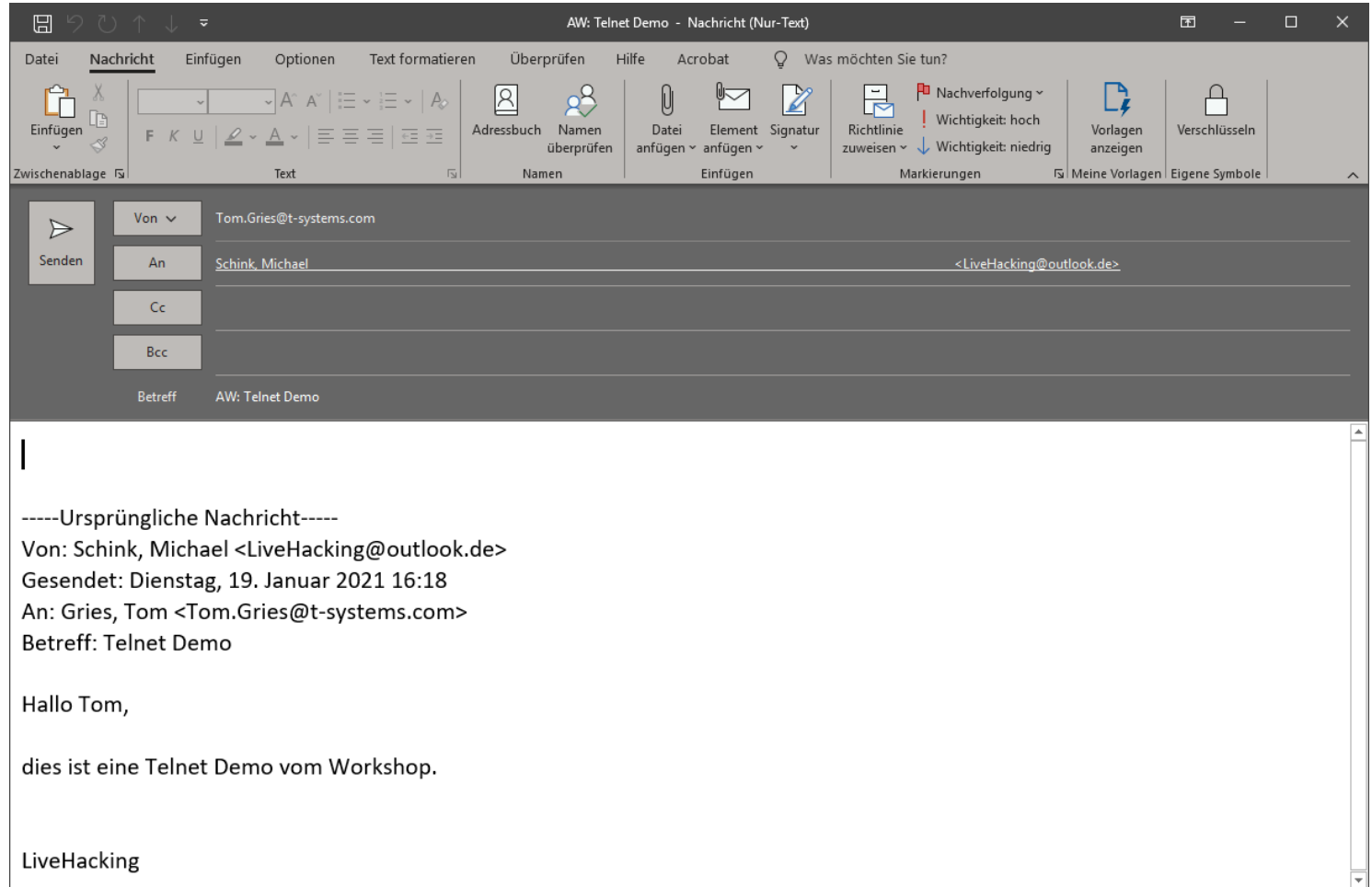


Mailversand mit Telnet - Email Adresse verschleiern

Noch Demo 2:

Bei dem Trick mit Leerzeichen erkennt man im An-Feld, dass etwas nicht stimmt: Sehr viel Platz zwischen dem Namen und der Email-Adresse - die auch nicht zur internen Adresse passt.

Kann man das besser verstecken?



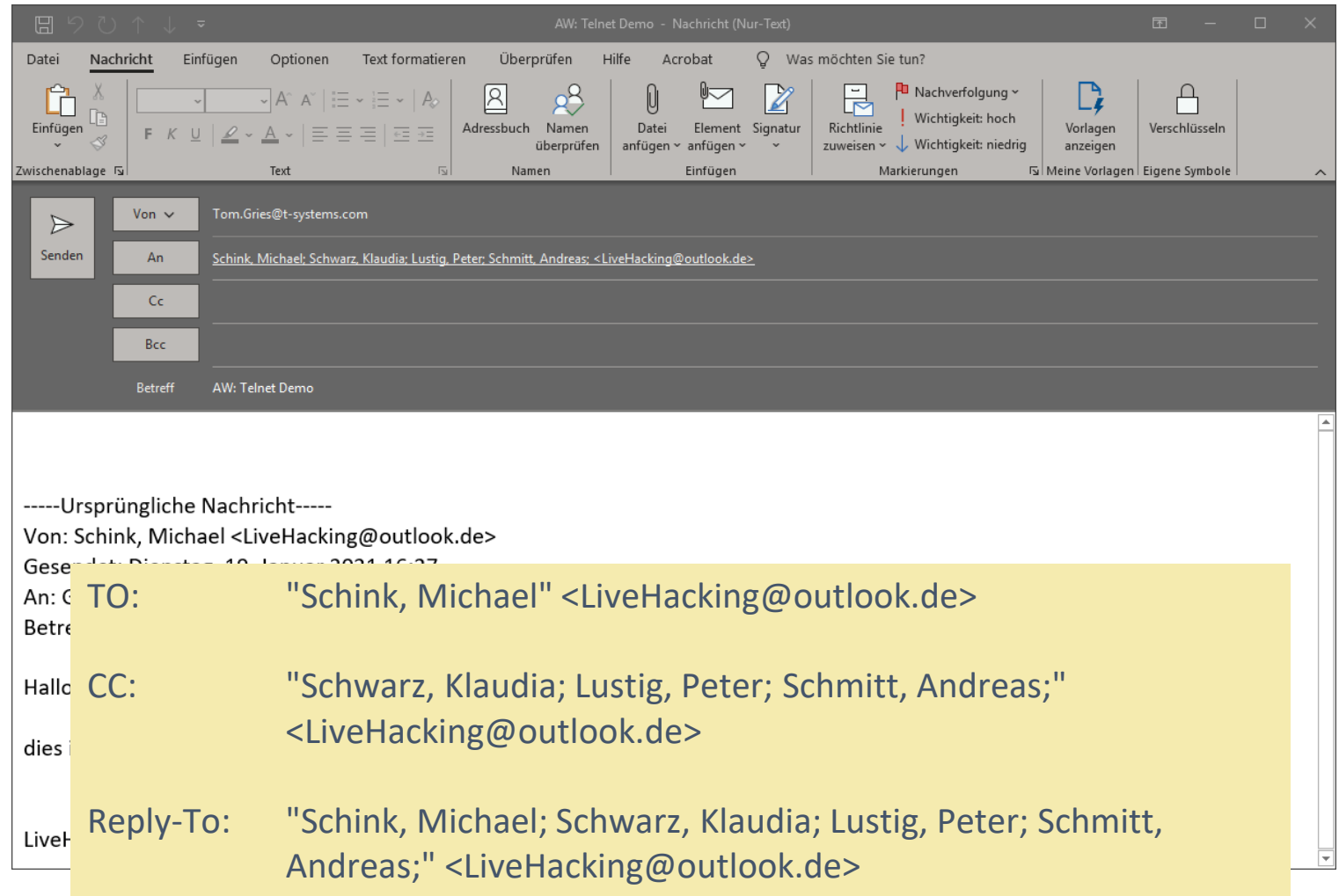


Mailversand mit Telnet - Email Adresse verschleiern

Demo 3:

In dieser Demo wurde das CC-Feld um ein paar Fantasie-Namen erweitert. Dadurch lässt sich die Emailadresse besser verstecken. Zusätzlich wurde ein "Reply-To" Feld angelegt.

Diese Antwort geht nur an LiveHacking@outlook.de.





Transportieren und Verteilen von Mails

MUA

Mail User Agent

Programm zum Empfangen, Lesen, Schreiben und Versenden von Mails.

MTA

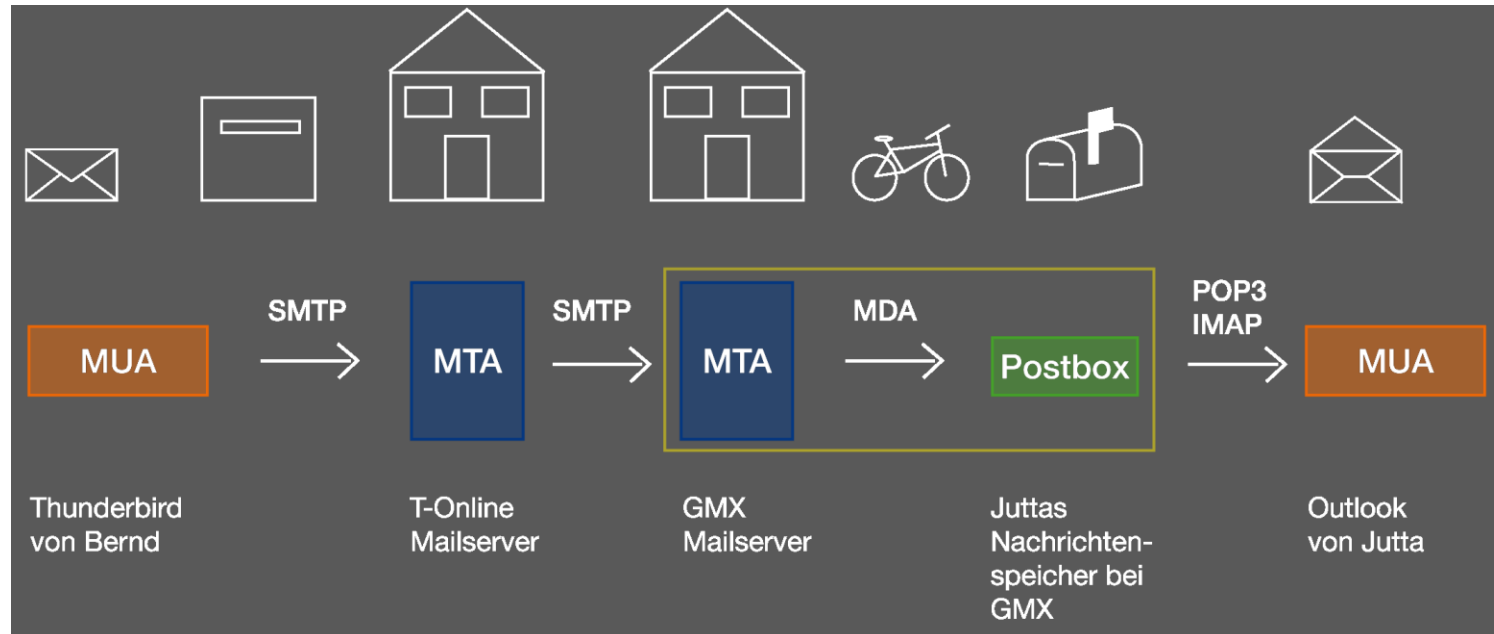
Mail Transfer Agent

Programm zum Transportieren und Verteilen von Mails.

MDA

Mail Delivery Agent

Programm zur Filterung und Verteilung von Mails in Mailboxen.



Anmerkungen oder Fragen?