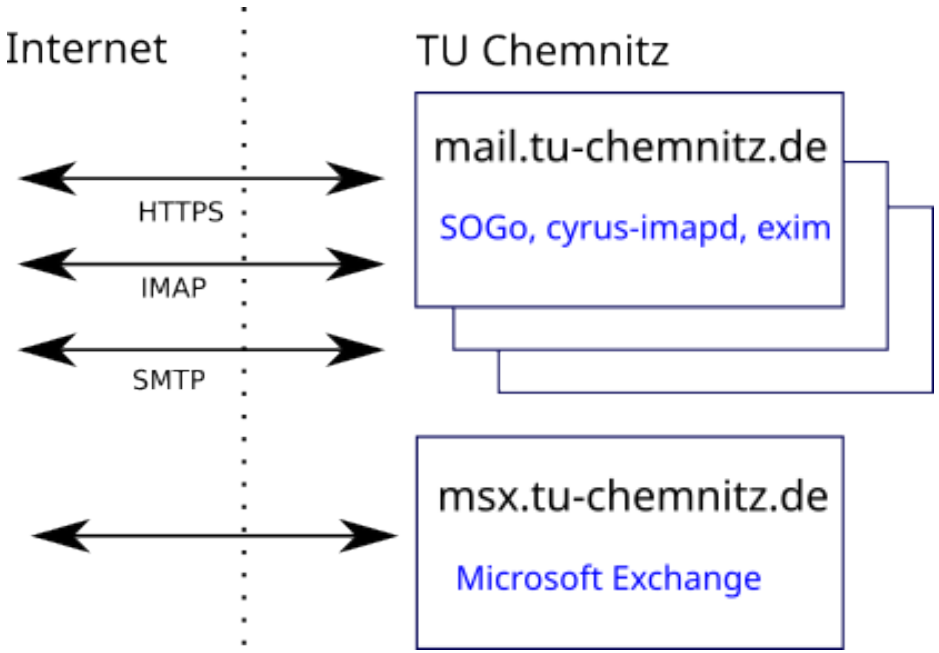
E-Mail-Zugang absichern – Wege zum 2. Faktor

Frank Richter

Technische Universität Chemnitz – Universitätsrechenzentrum

85. DFN-Betriebstagung – Berlin, 6. Oktober 2026

Ausgangspunkt bis November 2023



Aus dem Internet erreichbar:

- IMAP/POP3, SMTP – ca. 3.000 von 15.000 Benutzer/innen
- Webmail (HTTPS), CalDAV, CardDAV
- Exchange
- nur mit TLS und AUTH (Login, Passwort) – kein 2. Faktor

Vorfälle

- sicherheitskritische Software-Fehler
- täglich mehrere hunderttausende Brute-Force-Versuche
- Missbrauch durch Kompromittierung von Zugangsdaten durch Phishing, Malware . . .
  - 2024: 12 Vorfälle, 2025 bis Februar: 4
  - Spamversand: viel lästige Arbeit und Beeinträchtigungen
  - illegaler Zugriff auf E-Mail weitestgehend unbekannt

Gefährdet sind:

- persönlicher Datenschutz, Geschäftsgeheimnisse
- Reputation durch massenweisen Spamversand

→ bei kritischer Personalsituation!

Microsoft Exchange

- E-Mail für ca. 1.500 Mitarbeiter/innen (u. a. Rektorat, Verwaltung)
- zusätzlich 1.000 für Kalender
- Outlook, OWA, CalDAV

... unter dem (Ein)Druck von

- Cyber-Vorfällen an der TU Freiberg und WH Zwickau
- und einiger Zero-Day-Lücken

→ **seit 12 / 2023: Zugang nur noch aus dem Campusnetz / VPN**

- Blogartikel: mytuc.org/bghj
- gestützt durch Rektoratsbeschluss

- . . . fast nichts, beherrschbare Menge an Supportanfragen
- Nutzer durch Home-Office an VPN gewöhnt
- Problem Smartphone: eduVPN rettet :-)

2024: Multi-Faktor-Authentisierung

- www.tu-chemnitz.de/urz/idm/services/mfa.html
- mit eduMFA
- TOTP, Hardware-Token, TAN-Liste
- für IdP („Web-Trust-Center“) und VPN

→ Kraftakt: viel Support!

Maßnahmen für zentralen Mailbox-Server – Überlegungen

- E-Mail-Postfächer für ca. 13.500 Benutzer/innen
- IMAP, POP3, SMTP, Webmail (SOGo)

- E-Mail-Postfächer für ca. 13.500 Benutzer/innen
- IMAP, POP3, SMTP, Webmail (SOGo)

Überlegungen

1. Lokalen Maildienst abschaffen, outsourcen
   - (damals) nicht durchsetzbar

- E-Mail-Postfächer für ca. 13.500 Benutzer/innen
- IMAP, POP3, SMTP, Webmail (SOGo)

Überlegungen

1. Lokalen Maildienst abschaffen, outsourcen
   - (damals) nicht durchsetzbar
2. Mail-Login ausschließlich mit Zertifikaten
   - Aufwand sehr hoch für Nutzer und Support
   - viele technische Fragezeichen
   - Wie Webmail?

3. Verbesserung von technischen Schutzmaßnahmen
   - Überwachung von Nutzeraktivitäten – mit KI!
   - verschärfte Ratelimits
   - explizites Freischalten für IMAP, SMTP von extern

   $\rightarrow$ komplex für Nutzer und Administration, Erfolg fraglich

3. Verbesserung von technischen Schutzmaßnahmen
   - Überwachung von Nutzeraktivitäten – mit KI!
   - verschärfte Ratelimits
   - explizites Freischalten für IMAP, SMTP von extern

   $\rightarrow$ komplex für Nutzer und Administration, Erfolg fraglich

4. App- und Gerätepasswörter
   - bereits im IdM umgesetzt, für 15% der Mail-Nutzer in Verwendung
   - Hoffnung: werden nicht gemerkt, notiert, eingetippt – kein Phishing
   - … sondern gespeichert, dadurch anfällig für Malware
   - (war) Standardverfahren bei vielen Anbietern
   - an sich einfach, aber für 12.000 Benutzer einmalige Aktion
   - unsere Umsetzung verbesserungswürdig (expire)
   - Erfolg fragwürdig, aber intern hart diskutiert

5. OAUTH2 – der technische Königsweg, ABER
   - keine Unterstützung durch Mailprogramme
   - in Thunderbird hard coded für Gmail, Microsoft …
   - mAuth: OAUTH2 profile for mail
   - SASL Passkey

   → alles Drafts, praktisch nicht einsetzbar

5. OAUTH2 – der technische Königsweg, ABER
   - keine Unterstützung durch Mailprogramme
   - in Thunderbird hard coded für Gmail, Microsoft …
   - mAuth: OAUTH2 profile for mail
   - SASL Passkey

   → alles Drafts, praktisch nicht einsetzbar

6. **Webmail (SOGo) über IdP authentifizieren**
   - damit **2. Faktor aus dem Internet**
   - Eigenentwicklung, damit SOGo Nutzer am IMAP-Server authentisieren kann:
     - IdP erzeugt JWT mit expire, das nutzt SOGo als Passwort, IMAP-Server prüft via PAM
   - Sicherheit mit Komfort :-) mit kleinem aber

   → **seit 03/2025 in Betrieb:** mytuc.org/dqgk

7. IMAP/POP3/SMTP-Server hinter die Firewall

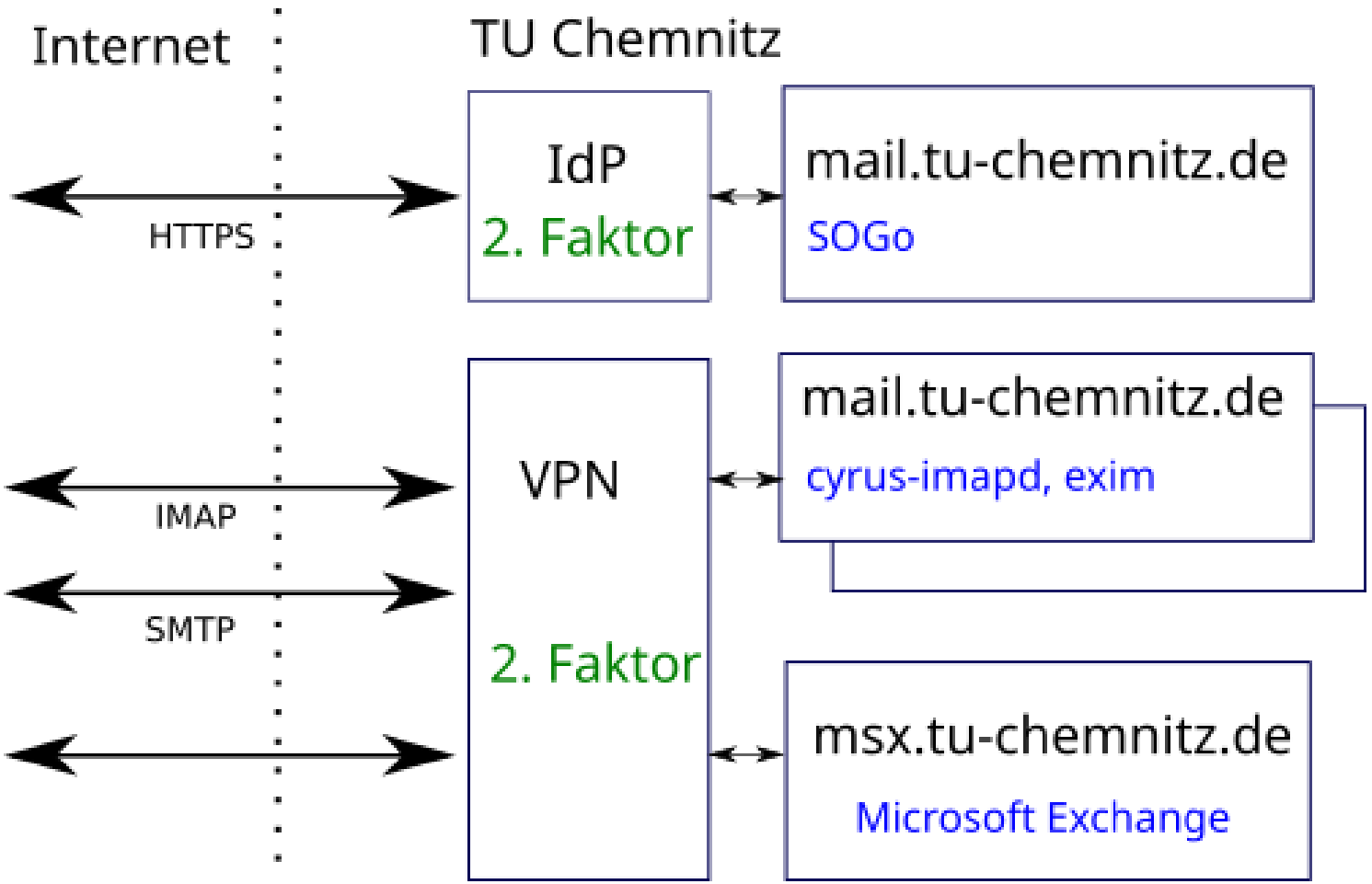
- nur noch aus dem Campusnetz / VPN
- damit **2. Faktor aus dem Internet**
- konsistent zu Exchange
- Schutz vor DDOS und Brute-Force-Attacken
- wenige Ausnahmen für externe Services (SMTP AUTH)
- Gegenargumente / Einwände – hart diskutiert:
  - unbequem: „lese keine Mails mehr von unterwegs“
  - „VPN lutscht Akku leer“
  - „macht sonst niemand“
  - „richte mir Weiterleitung an private Mailbox ein“

7. IMAP/POP3/SMTP-Server hinter die Firewall

- nur noch aus dem Campusnetz / VPN
- damit **2. Faktor aus dem Internet**
- konsistent zu Exchange
- Schutz vor DDOS und Brute-Force-Attacken
- wenige Ausnahmen für externe Services (SMTP AUTH)
- Gegenargumente / Einwände – hart diskutiert:
  - unbequem: „lese keine Mails mehr von unterwegs“
  - „VPN lutscht Akku leer“
  - „macht sonst niemand“
  - „richte mir Weiterleitung an private Mailbox ein“
- Entscheidung in Leitung absichern lassen
- Blogartikel: mytuc.org/mailvpn
- (betroffene) Nutzer zweimal angeschrieben
- IMAP ALERT bei externen Zugriffen eine Woche vorher

→ **seit 09/2025 in Betrieb**

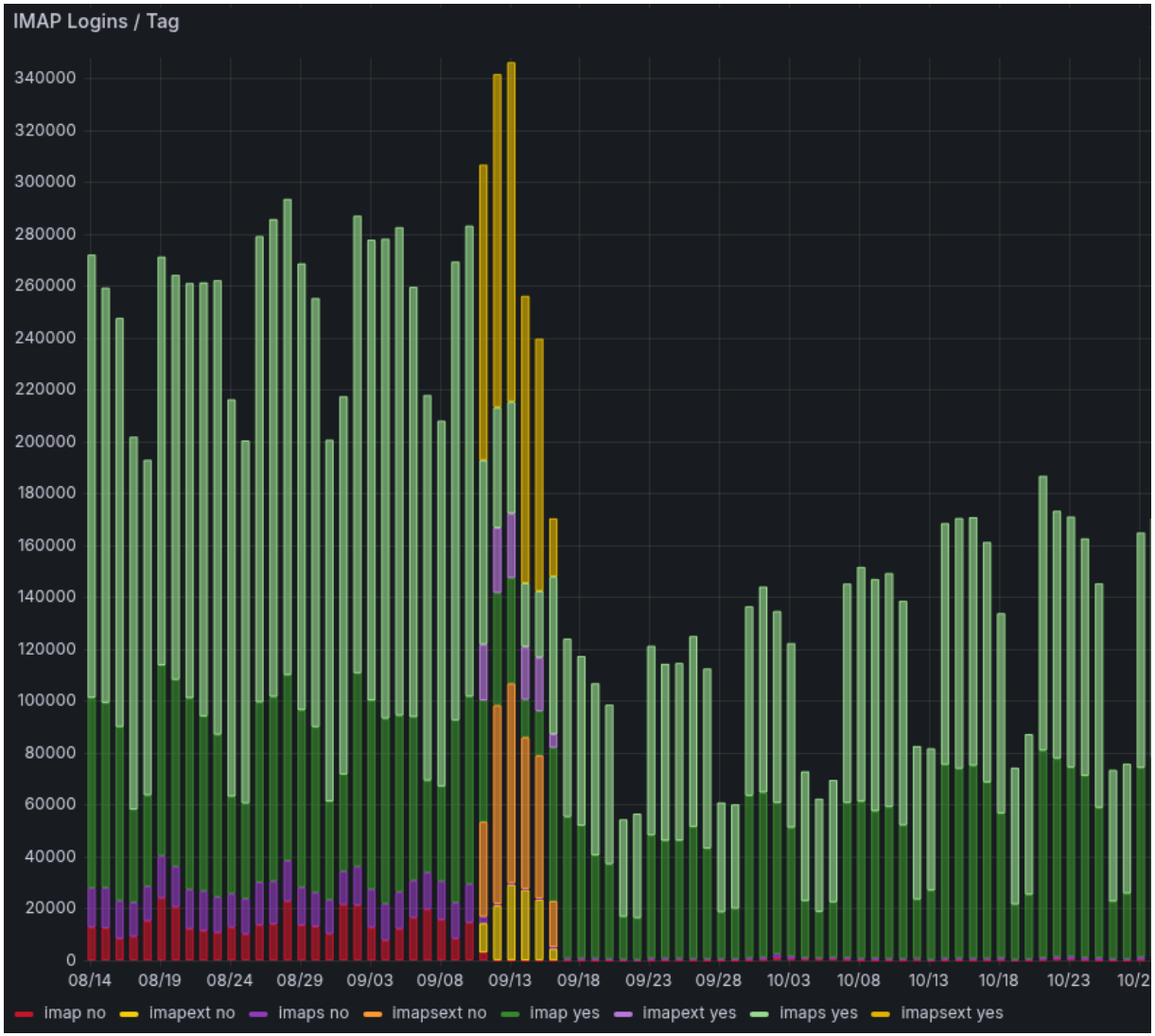
Zielzustand: 2. Faktor für E-Mail



→ Alle Zugriffe aus dem Internet mit 2. Faktor ✓

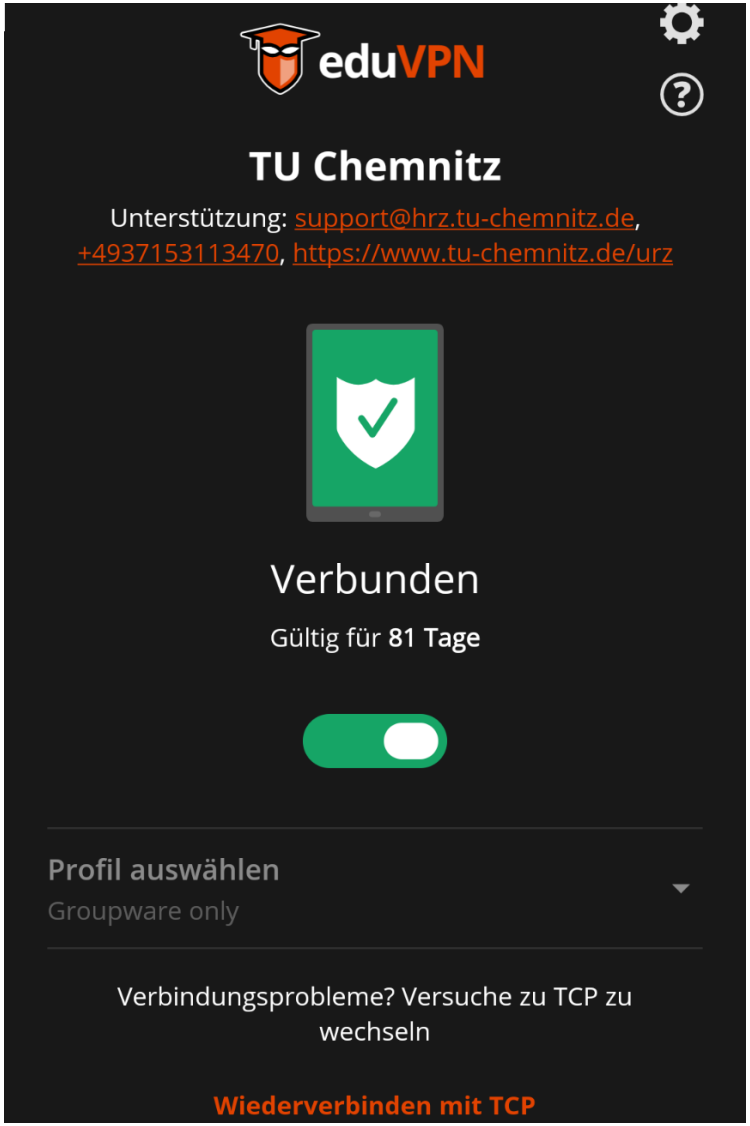
Was danach geschah

- Zugriffe sinken, insb. fehlerhafte Login-Versuche:



Fazit

- Komforteinbuße:
  - eduVPN ist der Retter
  - Profil „Groupware only“



Fazit

- „Flucht“ in Weiterleitungen
  - für Studierende ok, für Mitarbeiter/innen nicht geregelt
  - leider kein vorher-nachher erhoben

Fazit

- „Flucht“ in Weiterleitungen
  - für Studierende ok, für Mitarbeiter/innen nicht geregelt
  - leider kein vorher-nachher erhoben
- **Missbrauch von E-Mail-Accounts**

Fazit

- „Flucht“ in Weiterleitungen
  - für Studierende ok, für Mitarbeiter/innen nicht geregelt
  - leider kein vorher-nachher erhoben
- **Missbrauch von E-Mail-Accounts**
  - seit Einführung vor einem Jahr: **0**

Fragen / Diskussion

Fragen / Diskussion

- Wer hat DMARC `p=reject`
- Wer bietet JMAP-Server an?