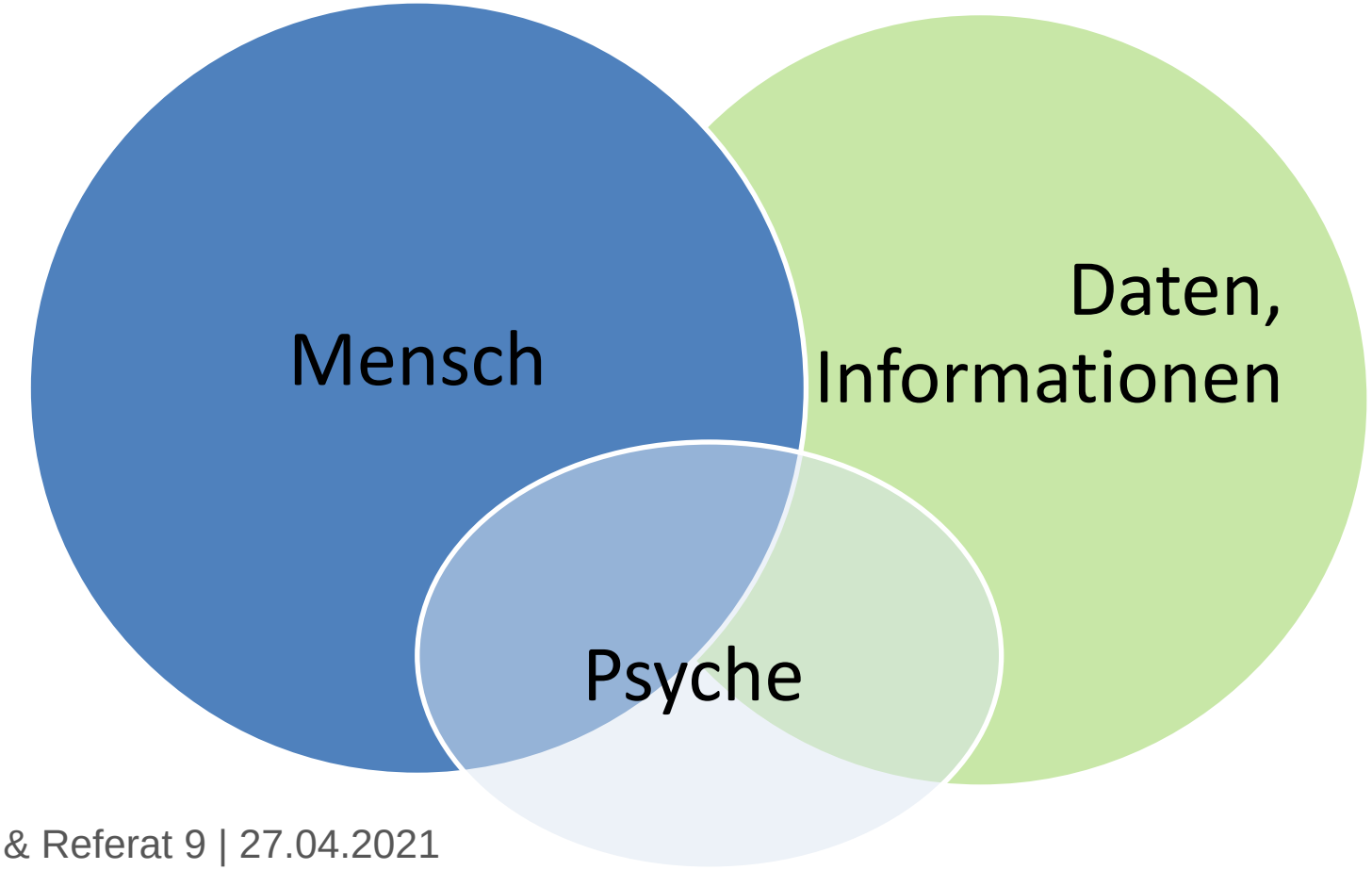
# Social Engineering erkennen und abwehren



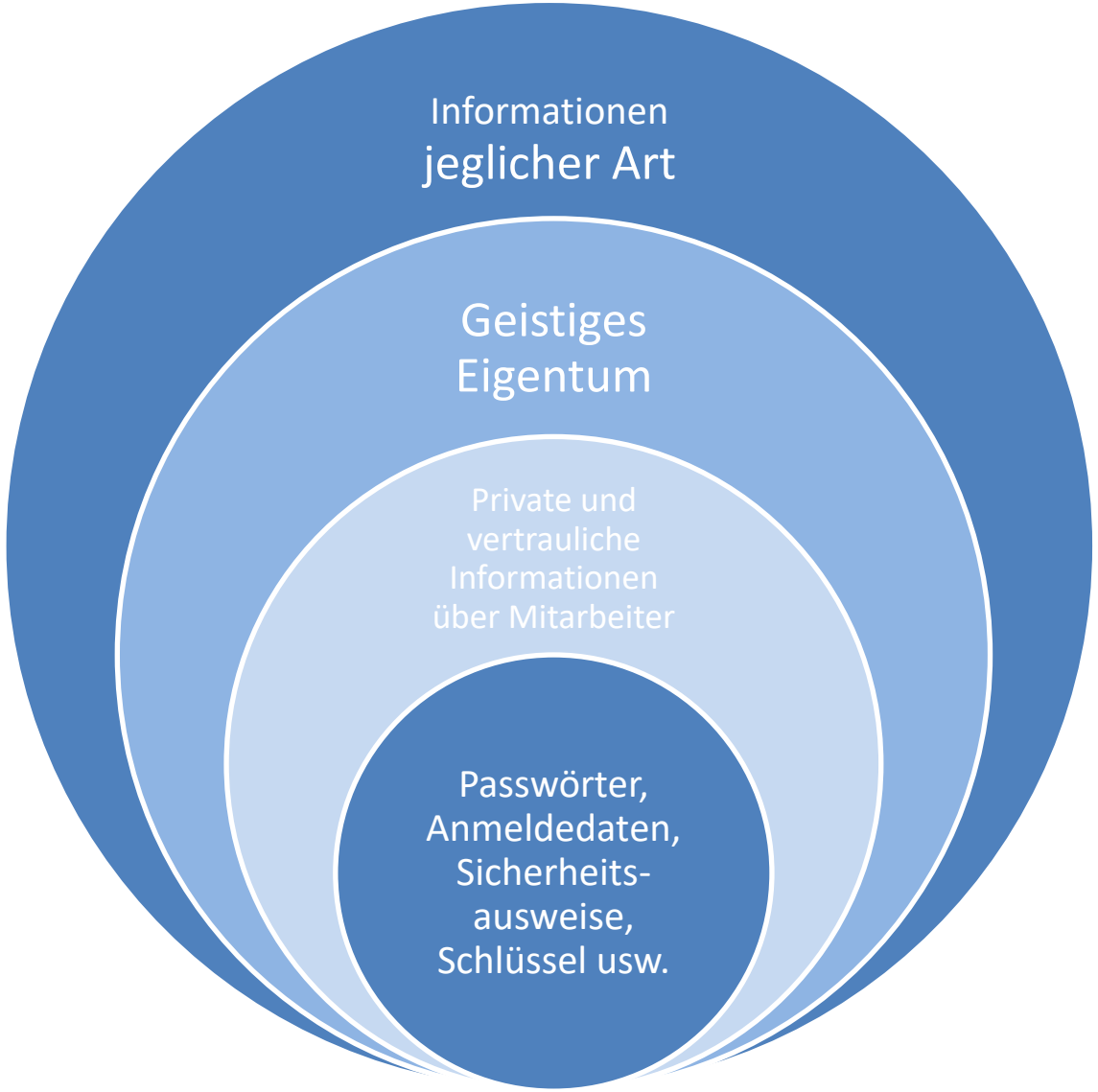

# Was ist Social Engineering?



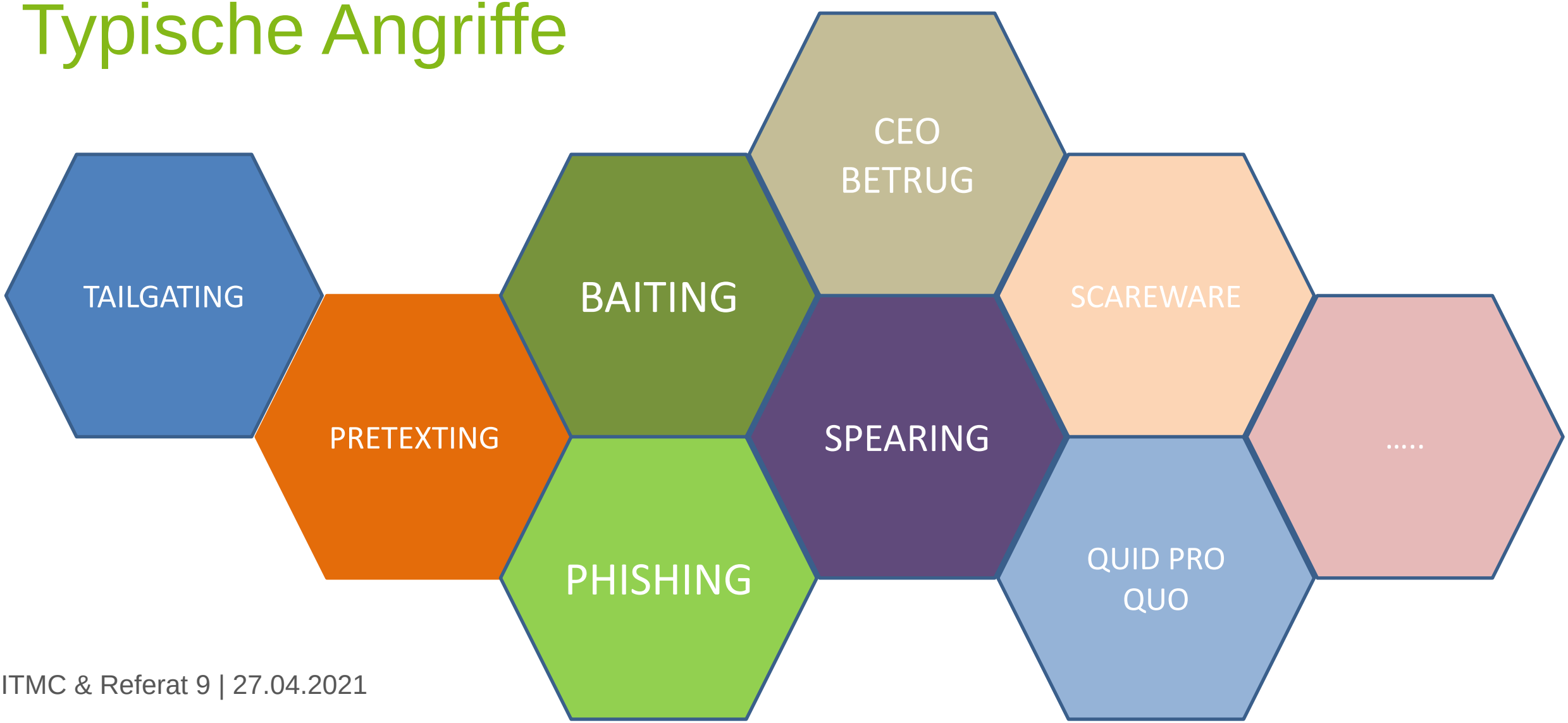

Social Engineering ist der Oberbegriff für eine Vielzahl von Methoden, die von Cyberkriminellen eingesetzt werden, um mit Hilfe von psychologischen Faktoren das Opfer zu manipulieren.

Ziel ist dabei, den Mensch als Einfallstor für den Angriff zu nutzen und ihn zu einer bestimmten Handlung (z. B. sensible Daten preis-geben, maliziösen Links folgen usw.) zu animieren.

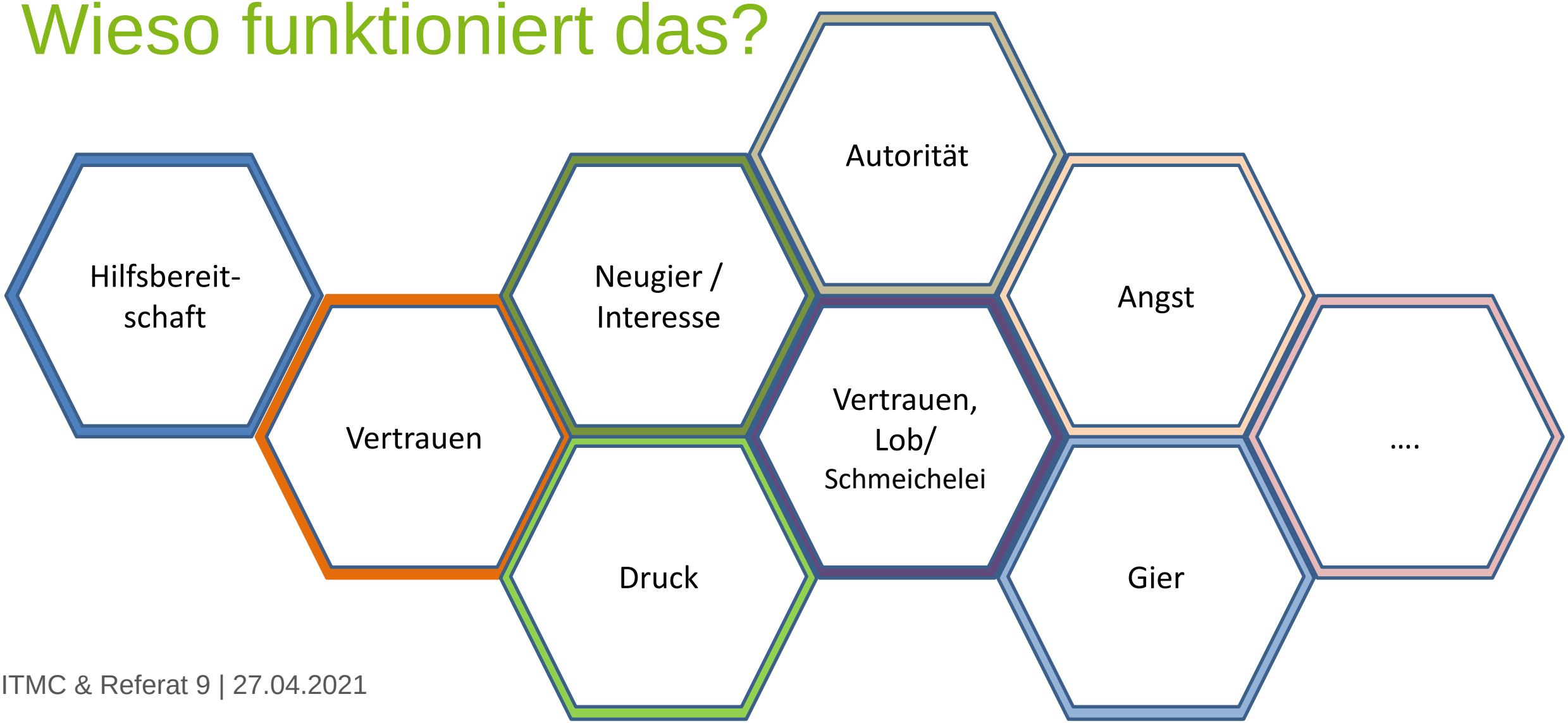
# Ziele


Informationen
jeglicher Art
Geistiges
Eigentum
Private und
vertrauliche
Informationen
über Mitarbeiter
Passwörter,
Anmeldedaten,
Sicherheits-
ausweise,
Schlüssel usw.

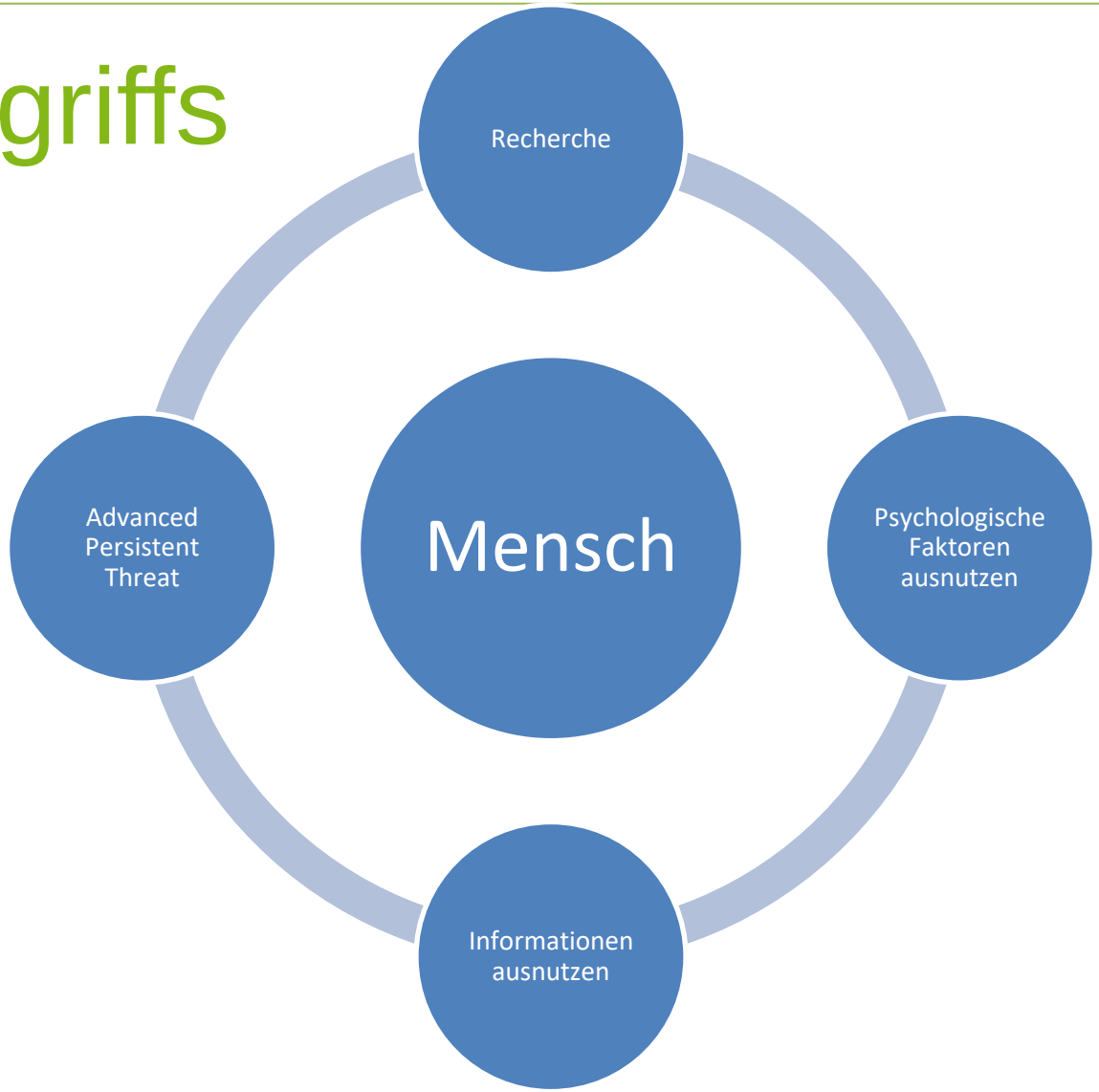
# Typische Angriffe



# Wieso funktioniert das?



# Zyklus eines SE-Angriffs

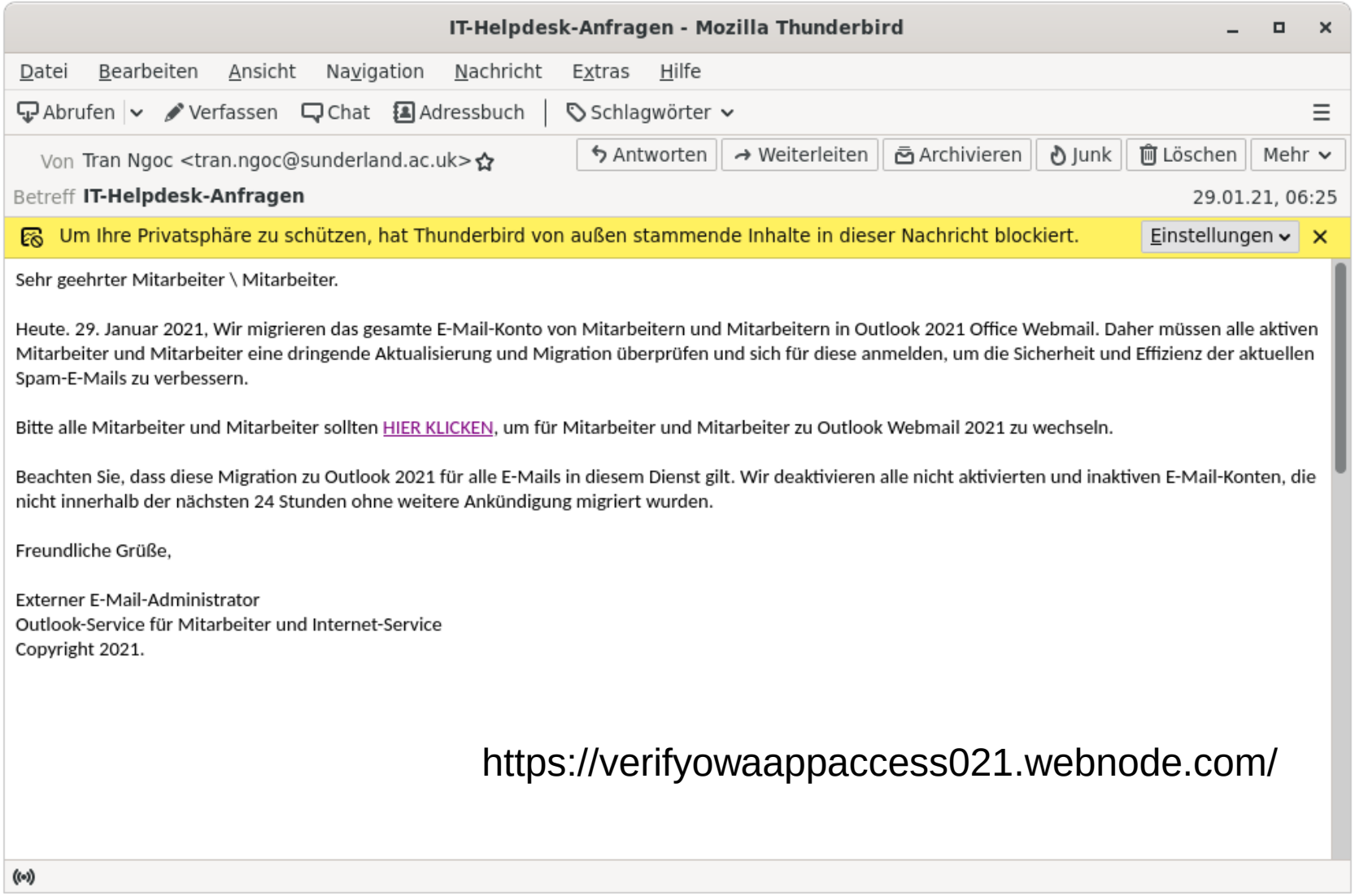


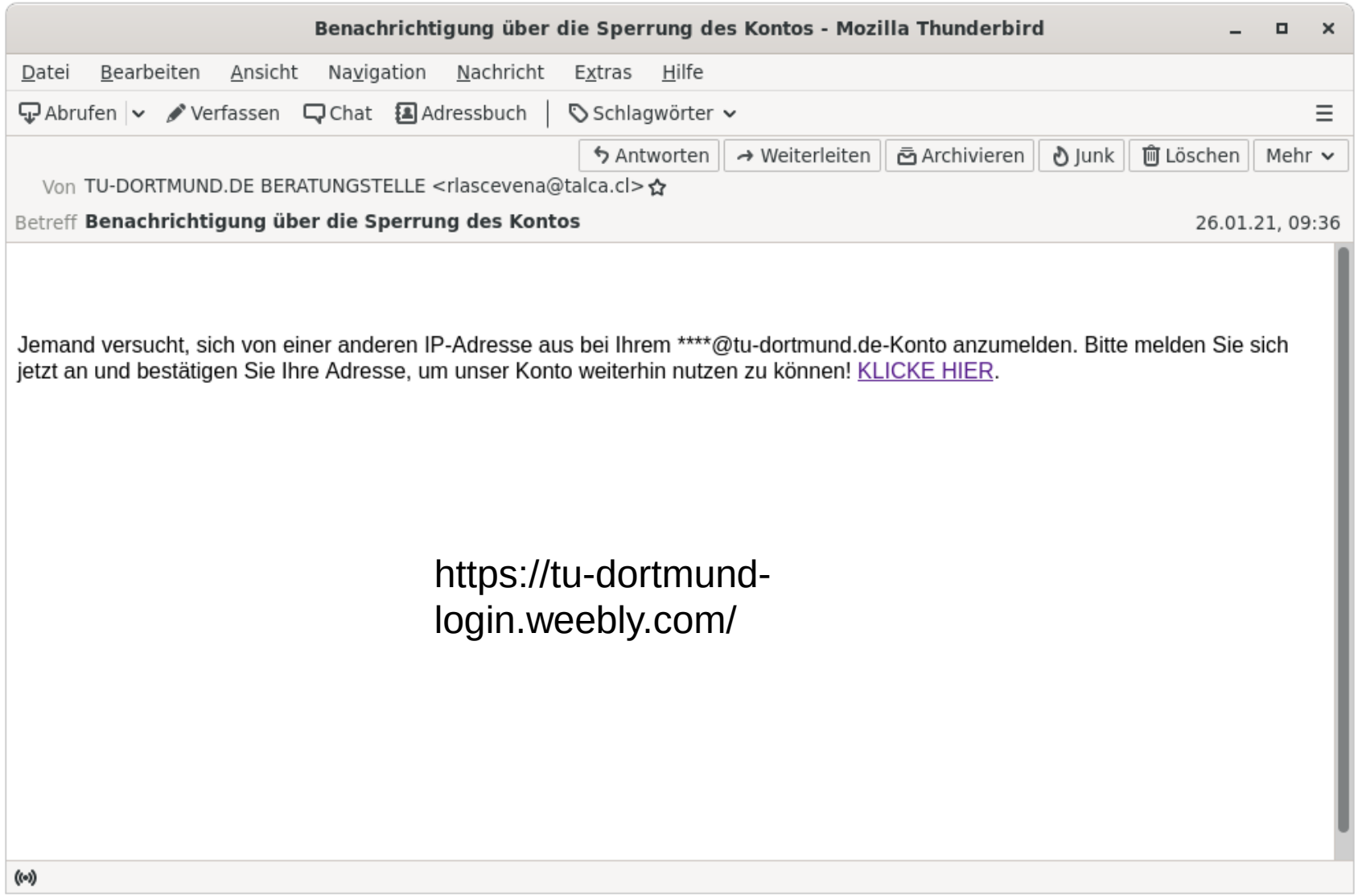
# Aktuelle Phishing Vorkommnisse an der TU

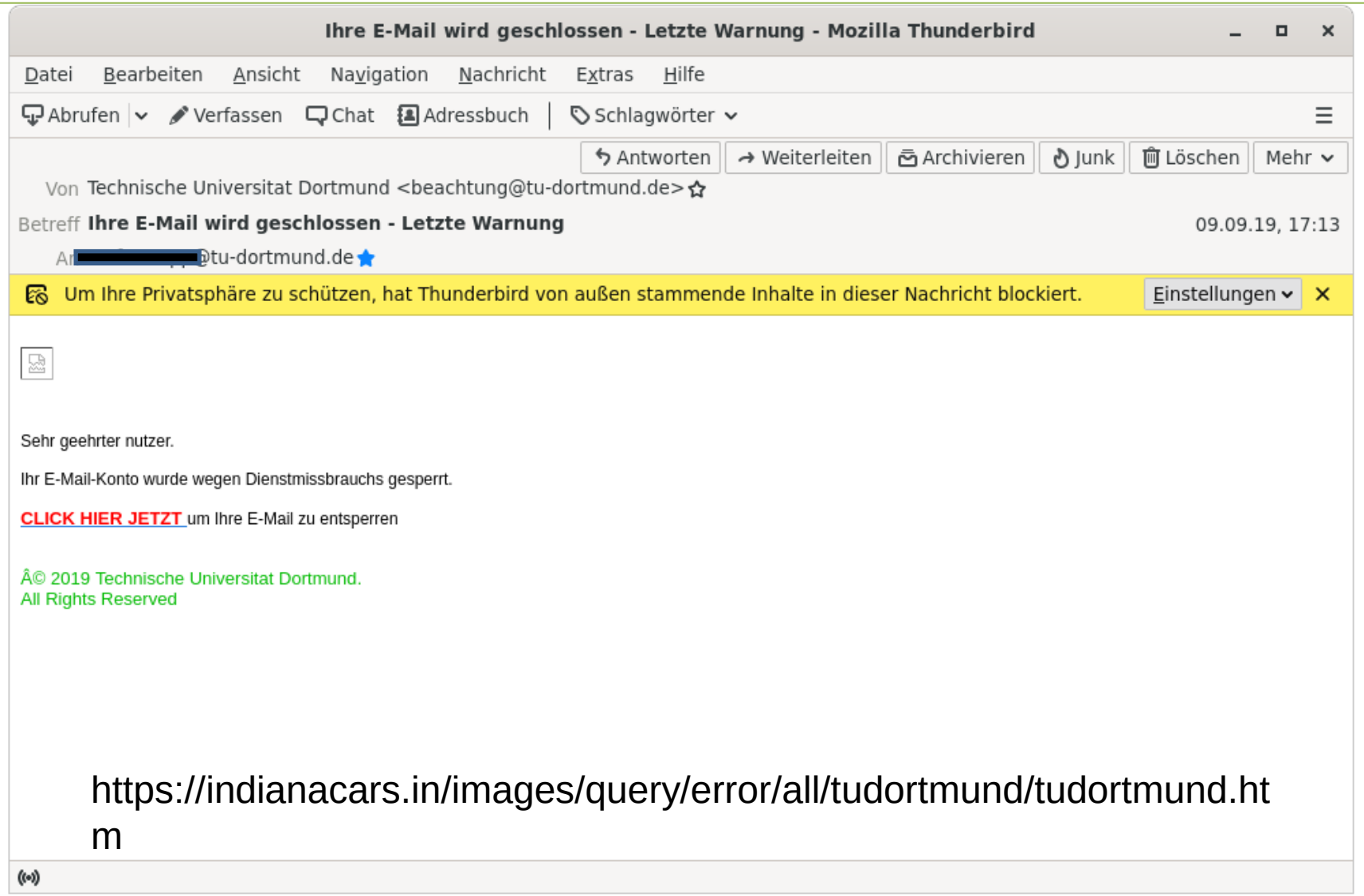
- Mails im Zusammenhang mit Postfächern
- Zahlungsanweisungen im Namen von Vorgesetzten
- Bewerbungen mit Schadsoftware im Anhang
- Mails mit Schadsoftware im Anhang, die reale Mails zitieren (aus gehackten Mailkonten)

# Erkennungsmerkmale

- Verweis auf Zeitdruck, Gewinne, Autoritäten
- Fehlerhaftes Deutsch oder Grammatik
- Ungewöhnliche Absender-Angaben oder Signatur
- Externer Link (evtl. verschleiert) oder (aktiver) Anhang


IT-Helpdesk-Anfragen - Mozilla Thunderbird
Datei Bearbeiten Ansicht Navigation Nachricht Extras Hilfe
Abrufen Verfassen Chat Adressbuch Schlagwörter
Von Tran Ngoc <tran.ngoc@sunderland.ac.uk>
Antworten Weiterleiten Archivieren Junk Löschen Mehr
Betreff IT-Helpdesk-Anfragen
29.01.21, 06:25
Um Ihre Privatsphäre zu schützen, hat Thunderbird von außen stammende Inhalte in dieser Nachricht blockiert.
Einstellungen
Sehr geehrter Mitarbeiter \ Mitarbeiter.
Heute. 29. Januar 2021, Wir migrieren das gesamte E-Mail-Konto von Mitarbeitern und Mitarbeitern in Outlook 2021 Office Webmail. Daher müssen alle aktiven Mitarbeiter und Mitarbeiter eine dringende Aktualisierung und Migration überprüfen und sich für diese anmelden, um die Sicherheit und Effizienz der aktuellen Spam-E-Mails zu verbessern.
Bitte alle Mitarbeiter und Mitarbeiter sollten HIER KLICKEN, um für Mitarbeiter und Mitarbeiter zu Outlook Webmail 2021 zu wechseln.
Beachten Sie, dass diese Migration zu Outlook 2021 für alle E-Mails in diesem Dienst gilt. Wir deaktivieren alle nicht aktivierten und inaktiven E-Mail-Konten, die nicht innerhalb der nächsten 24 Stunden ohne weitere Ankündigung migriert wurden.
Freundliche Grüße,
Externer E-Mail-Administrator
Outlook-Service für Mitarbeiter und Internet-Service
Copyright 2021.
https://verifyowaappaccess021.webnode.com/


Benachrichtigung über die Sperrung des Kontos - Mozilla Thunderbird
Datei Bearbeiten Ansicht Navigation Nachricht Extras Hilfe
Abrufen Verfassen Chat Adressbuch Schlagwörter
Antworten Weiterleiten Archivieren Junk Löschen Mehr
Von TU-DORTMUND.DE BERATUNGSTELLE <rlascevena@talca.cl>
Betreff Benachrichtigung über die Sperrung des Kontos
26.01.21, 09:36
Jemand versucht, sich von einer anderen IP-Adresse aus bei Ihrem ****@tu-dortmund.de-Konto anzumelden. Bitte melden Sie sich jetzt an und bestätigen Sie Ihre Adresse, um unser Konto weiterhin nutzen zu können! KLICKE HIER.
https://tu-dortmund-login.weebly.com/




https://indianacars.in/images/query/error/all/tudortmund/tudortmund.htm

# Was hilft gegen Social Engineering?

| Sicherheitsbewusstsein | Wissen | Verifizieren |
| --- | --- | --- |
| • Permanenter Prozess und kein einmaliges Doing<br>• Gesunde Skepsis gegenüber fremden Dritten<br>• Niemals dem Aufruf zur Übermittlung von persönlichen Daten folgen (PIN, Passwörter) folgen<br>• Seien Sie sparsam mit Auskünften | • Nutzen Sie unsere Informationsangebote zu unterschiedlichen Themen<br>• Informieren Sie sich über aktuelle Bedrohungen an der TU (https://itmc.tu-dortmund.de/das-itmc/meldungen-und-stoerungen/) | • Prüfen Sie immer die Identität des Bittstellers (Rufidentifikation, Rückruf, über Kollegen/Kolleginnen)<br>• Keine sensiblen Informationen an Personen weitergeben, die nicht als Informationsberech-tigte verifiziert sind |

Technik (z. B. Digitale Signaturen, Bildschirmsperre)

# Schnell-Check bei E-Mail-Eingang

- Kennen Sie den Absender?
- Erwarten Sie ein Dokument vom Absender?
- Weblink (URL!) plausibel?
- Klingt die Email plausibel? (Inhalt, Betreff)
- Absendermailadresse plausibel?

Wenn Sie alle Fragen nicht bejahen können, öffnen Sie keine Anhänge oder folgen Sie keinen Download-Links

- Befolgen Sie unsere Top Ten Tipps (unter https://service.tu-dortmund.de/group/intra/was-ist-phishing-)

# Empfohlene Vorgehensweise

Emails mit TU-Bezug im Anhang weiterleiten an:

- service.itmc@tu-dortmund.de
- alarm.sic@tu-dortmund.de

Melden Sie unerwünschte Mails wie Spam oder Phishing über das **Plug-In für Outlook** an unseren E-Mail Appliance. Weitere Infos unter: https://service.tu-dortmund.de/group/intra/spam-filterung

Hilfe bei Verdacht auf eine Kompromittierung:

- Trennen Sie den potentiell infizierten Rechner vom Netzwerk - Kontaktieren Sie uns unter alarm.sic@tu-dortmund.de für die weiteren Schritte.

# Digital signieren

- In Mailprogrammen über S/MIME (integriert) oder PGP (Plugin) verfügbar
- Persönliches Zertifikat als Voraussetzung
  - z.B. über Unicard mit Chipkartenleser
  - https://service.tu-dortmund.de/group/intra/nutzung-der-zertifikate

# Starke Passwörter

- Möglichst lang und schwer zu erraten
- Keine bekannten Wörter
- Mischung Klein-/Großbuchstaben, Ziffern, Sonderzeichen
- Möglichst unterschiedliche Passwörter für mehrere Dienste
- Nicht automatisch speichern. Passwortsafes bieten Hilfe.
- Bei Verdacht auf Identitätsdiebstahl Passwörter umgehend ändern
- Überprüfung, ob Mailadresse mit Passwort evtl. in Datenbanken auftaucht
  - https://haveibeenpwned.com/
  - https://leakchecker.uni-bonn.de