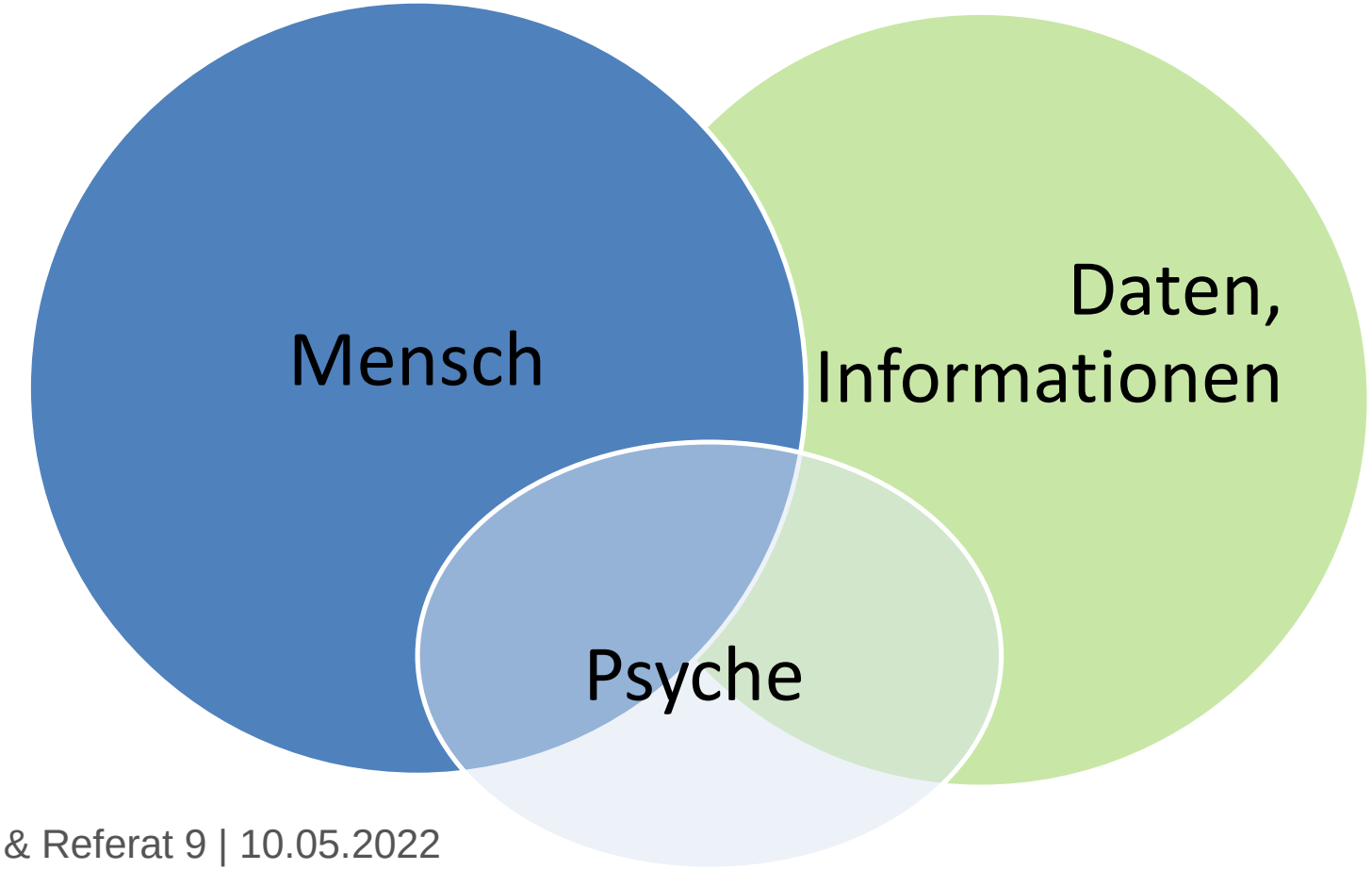
Security Awareness – Tipps und Tricks rund um Phishing und Co.

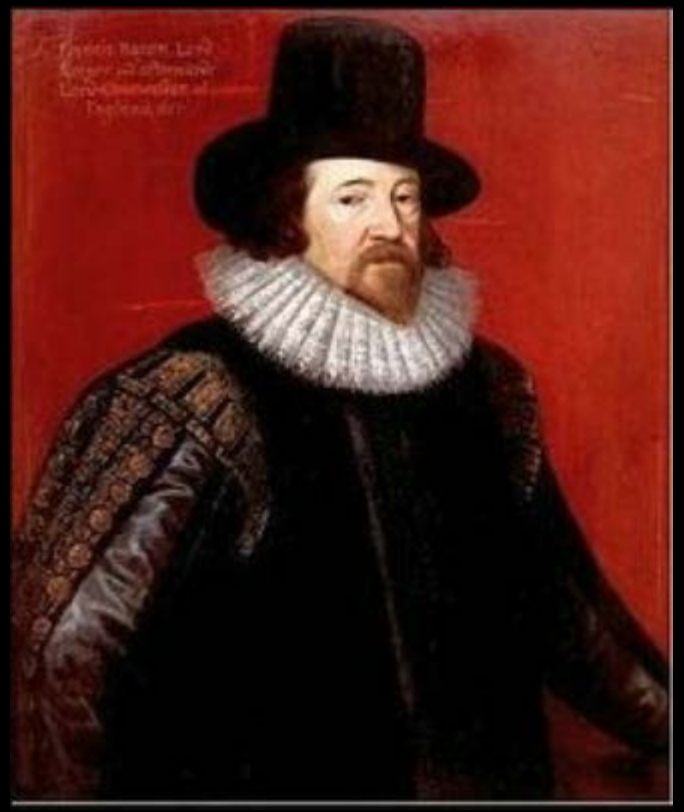
Was ist Social Engineering?



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.

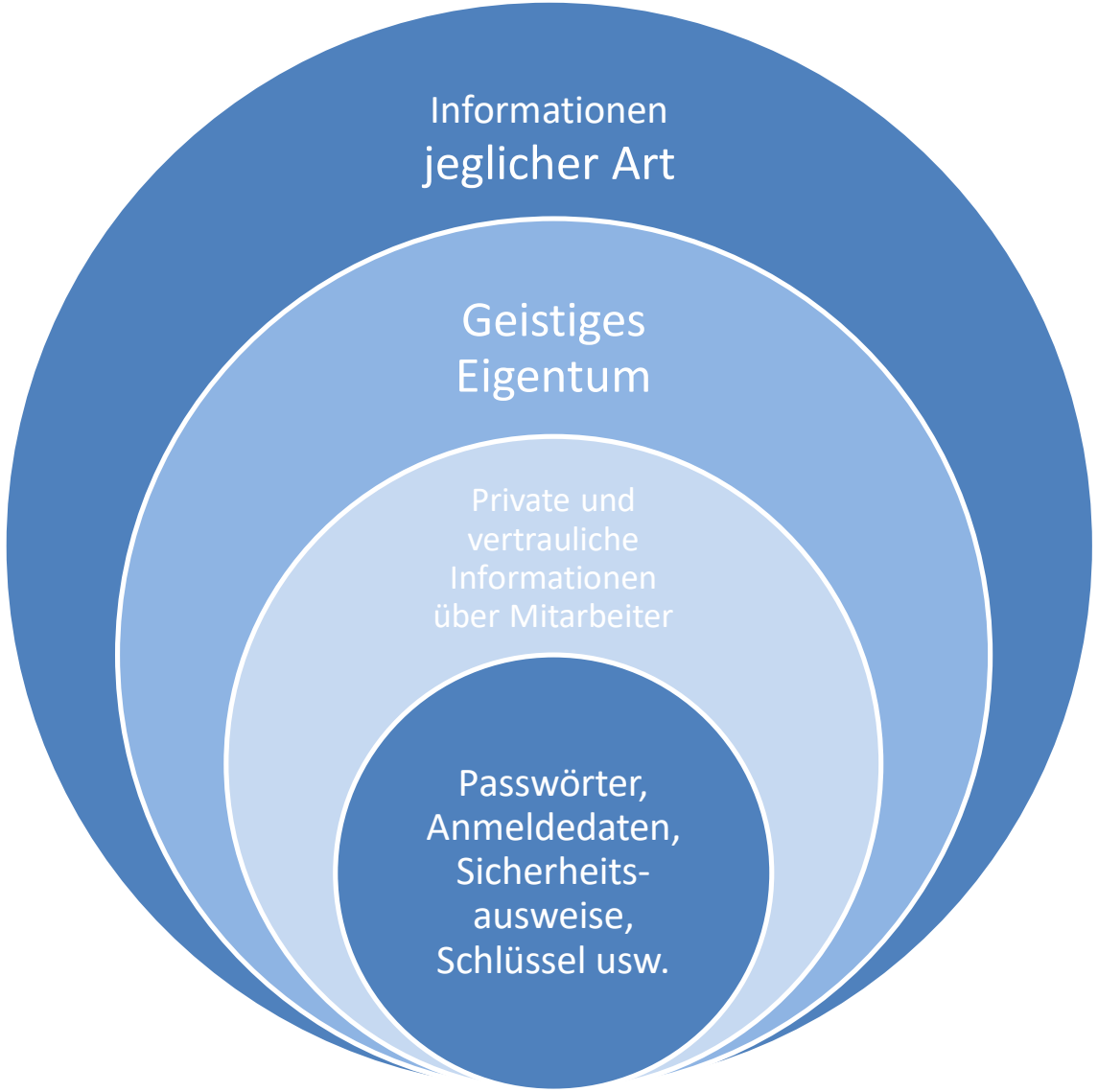
Warum?



„Denn Wissen selbst ist Macht“

(Francis Bacon 1561 - 1626)

Ziele des SE


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

Spearing

„ Ich habe aber nichts zu verbergen“

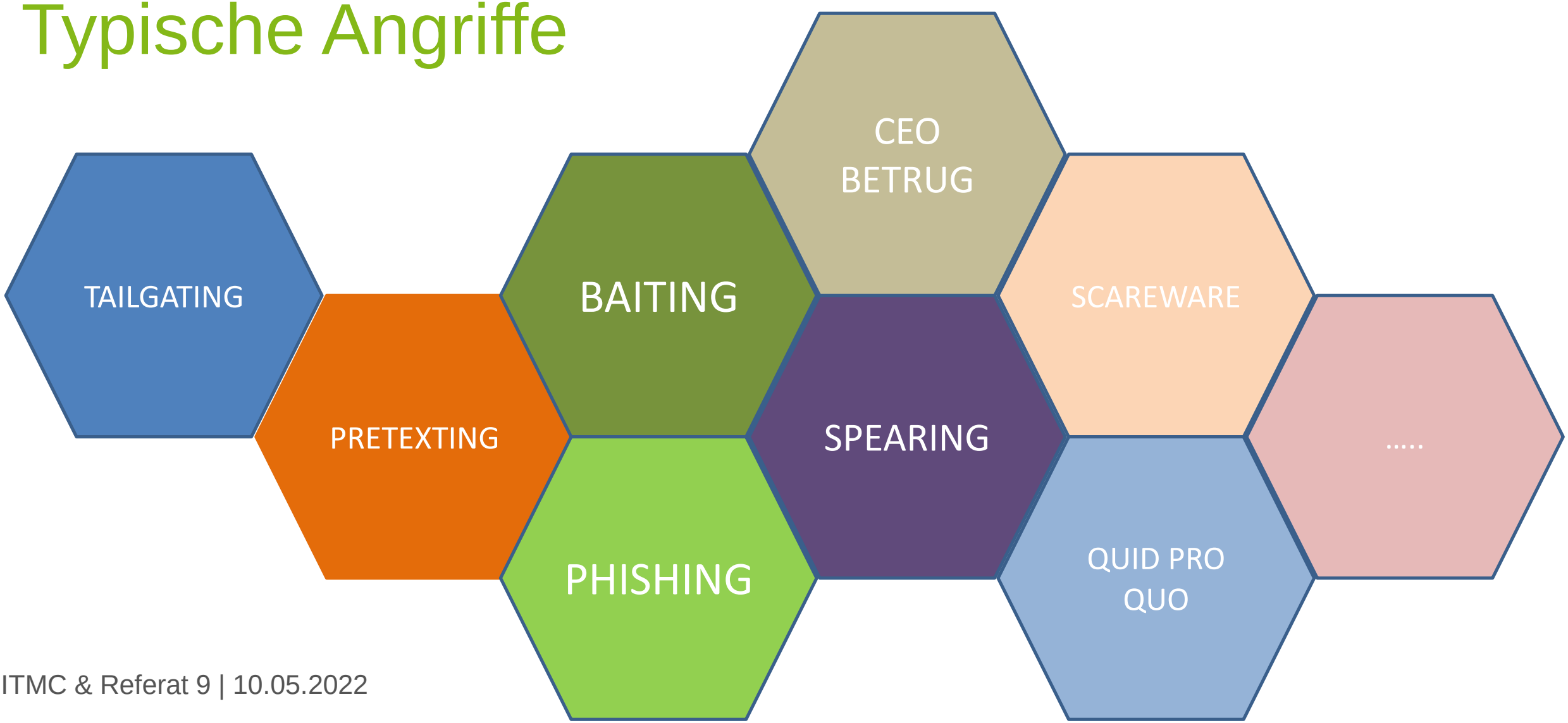
Sie sind das Hauptziel des Angriffs.

“

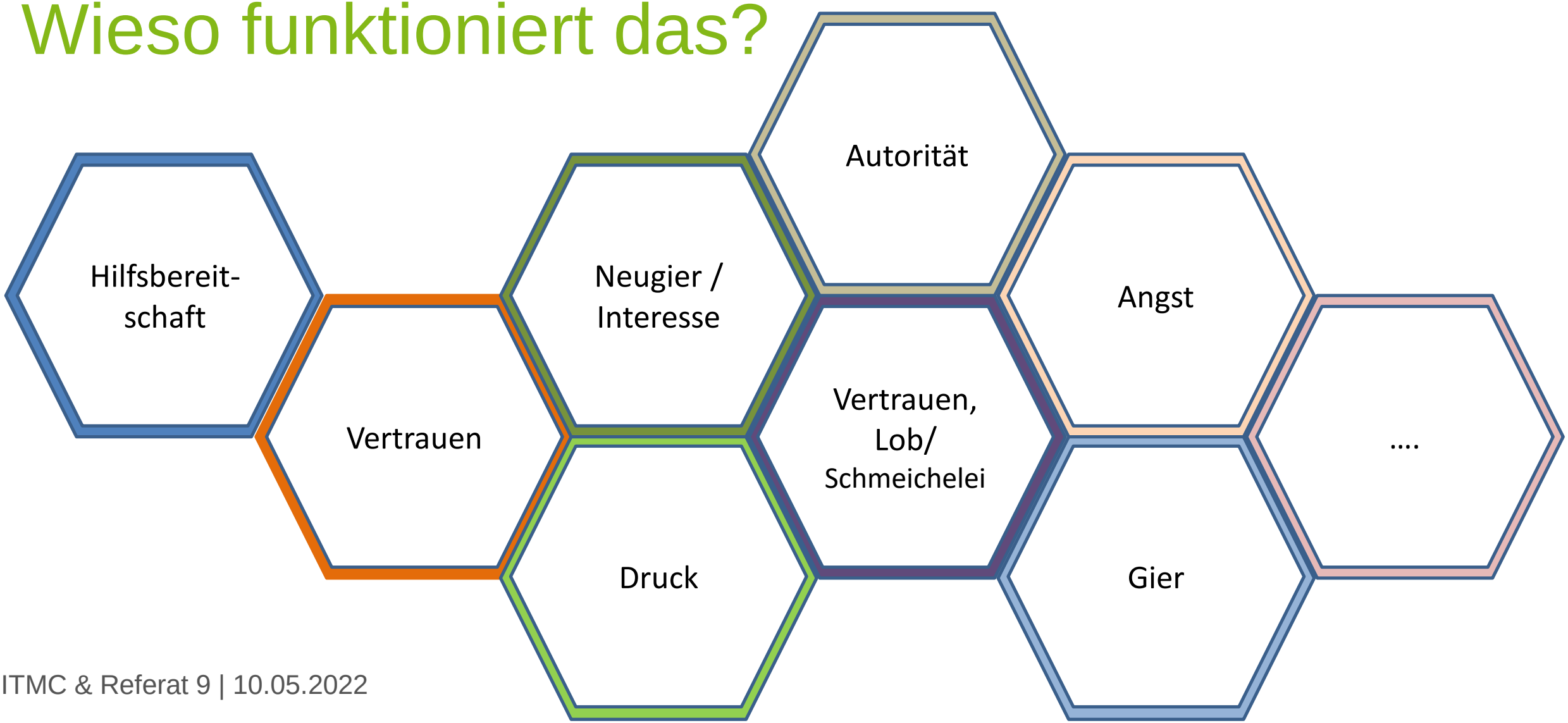
o d e r

Sie fungieren als Transportmittel bzw. Einfallstor.

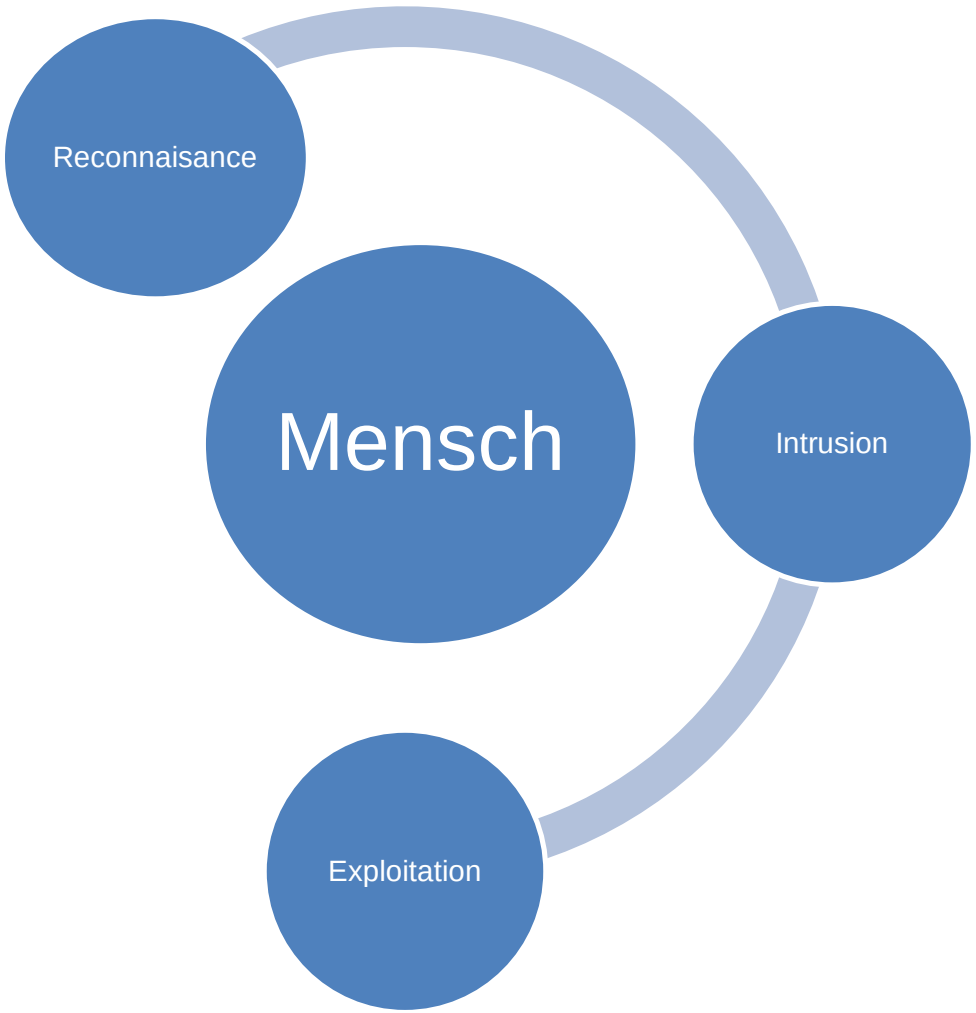
Typische Angriffe



Wieso funktioniert das?



Cyber-Killchain



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.

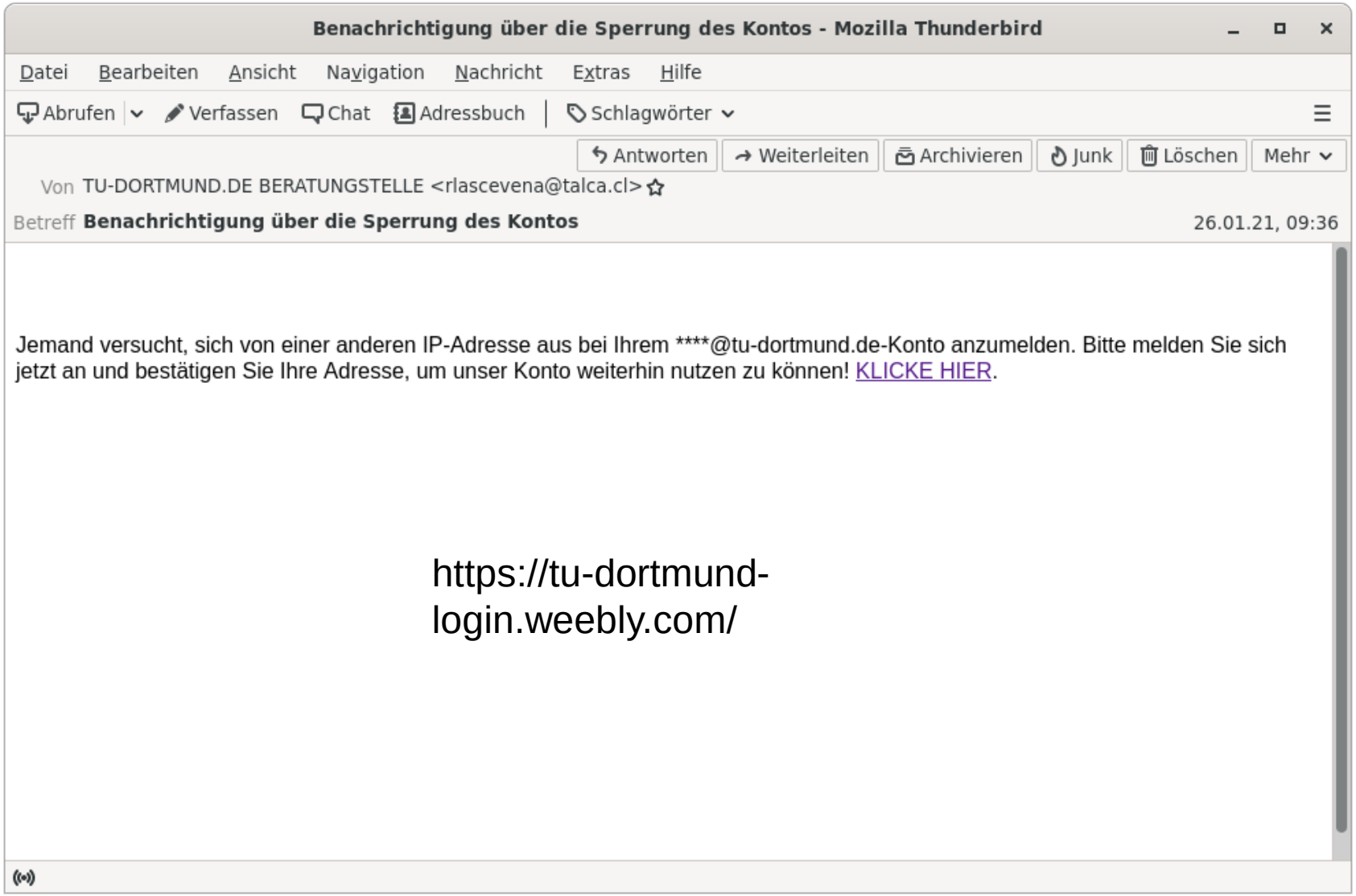
Bitte alle Mitarbeiter und Mitarbeiter sollten HIER KLICKEN, um für Mitarbeiter und Mitarbeiter zu Outlook Webmail 2021 zu wechseln.

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/



https://tu-dortmund-login.weebly.com/

Ihre E-Mail wird geschlossen - Letzte Warnung - Mozilla Thunderbird

Datei Bearbeiten Ansicht Navigation Nachricht Extras Hilfe

Abrufen Verfassen Chat Adressbuch Schlagwörter

Antworten Weiterleiten Archivieren Junk Löschen Mehr

Von Technische Universitat Dortmund <beachtung@tu-dortmund.de>

Betreff **Ihre E-Mail wird geschlossen - Letzte Warnung** 09.09.19, 17:13

An [redacted]@tu-dortmund.de

Um Ihre Privatsphäre zu schützen, hat Thunderbird von außen stammende Inhalte in dieser Nachricht blockiert. Einstellungen

Sehr geehrter nutzer.

Ihr E-Mail-Konto wurde wegen Dienstmissbrauchs gesperrt.

CLICK HIER JETZT um Ihre E-Mail zu entsperren

Â© 2019 Technische Universitat Dortmund.
All Rights Reserved

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

Was hilft gegen Social Engineering?

Sicherheitsbewusstsein	Wissen	Verifizieren
• Permanenter Prozess und kein einmaliges Doing • Lassen Sie Ihren Arbeitsplatz nicht unbeaufsichtigt • Gesunde Skepsis gegenüber fremden Dritten • Niemals dem Aufruf zur Übermittlung von persönlichen Daten folgen (PIN, Passwörter) folgen • Seien Sie sparsam mit Auskünften	• Nutzen Sie unsere Informationsangebote zu unterschiedlichen • Informieren Sie sich über aktuelle Bedrohungen an der TU (https://itmc.tu-dortmund.de/das-itmc/meldungen-und-stoerungen/)	• Prüfen Sie stets die Identität des Bittstellers (Rufidentifikation, Rückruf, über KollegInnen) • Keine sensiblen Informationen an Personen weitergeben, die nicht als berechtigt verifiziert wurde.

Technik (z. B. Digitale Signaturen, Bildschirmsperre uvm.)

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

Je länger, desto besser!

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

(siehe unter https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=tabletext, abgerufen am 03.05.2022)

Starke Passwörter

- Möglichst lang und schwer zu erraten, d.h. mindestens 8, besser 12 Zeichen
- Keine Wörter aus dem Wörterbuch
- Mindestens aus einem Klein-,Großbuchstaben, einer Ziffer, einem Sonderzeichen
- Möglichst unterschiedliche Passwörter für mehrere Dienste
- Nicht automatisch speichern. Passwortsafes mit einem Masterkey-Passwort bieten Hilfe.
- Bei Verdacht auf Identitätsdiebstahl Passwörter umgehend ändern

Hilfreiche Links zur Prüfung von Passwörtern

- Überprüfung, ob Mailadresse mit Passwort evtl. in Datenbanken auftaucht
  - https://haveibeenpwned.com/
  - https://leakchecker.uni-bonn.de

Wie stark ist mein Passwort?

  - https://nordpass.com/secure-password/

www.tu-dortmund.de