T.I.S.P. Community Meeting 2023

Berlin, 07. - 08.11.2023

Business Chat - frei von Phishing, Spoofing und Spam? Let's call it Chishing

Nick Lorenz, AWARE7

Unser Team - unsere Kompetenz

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Kreativer & professioneller Dienstleister in der IT-Security Branche

AWARE7
full service awareness agency

Penetrationstests & Sicherheitsuntersuchungen

- Mehr als 1.000 PT p.a.
- Internationale Kundschaft
- Exzellente Qualität & Expertise
- Zählen zu den größten Pentest Teams in NRW

Live Hacking & Cyber Security Shows

- Projektübergreifender Austausch
- von 30 bis 180 Minuten
- Im Duett und zweisprachig

IT-Sicherheitskonzeption ISO 27001

- Vom Beginn bis zur Zertifizierung
- Partner für internes und zert. Audit
- Bereitstellung von ext. ISBs

Individuelle IT-Security Projekte

- Aus- und Durchführung von individuellen Projekten
- Enge Zusammenarbeit mit Instituten, Fachhochschulen und Universitäten
- Publikationen in Top Konferenzen und Journals (PETS, WWW)

Wer bin ich?

Nick Lorenz, B.Sc.

Penetrationstester und Referent bei der AWARE7 GmbH

- **Fachinformatiker, Bachelor of Science und Master of Science**
  - Ausgebildeter Fachinformatiker für Systemintegration
  - Bachelor of Science in Informatik Spez. Informationssicherheit
  - Master of Sciene in Internet-Sicherheit (Aktuell)
- **OffSec Certified Professional (OSCP)**
- **IS-Penetrationstester**
- **Vorfall-Praktiker des BSI im Cyber-Sicherheitsnetzwerk**
- **TeleTrust Information Security Professional (T.I.S.P.)**
- **Project Leader und Lead-Author, zusammen mit Tim Barsch, der OWASP Top 10 Insider Threats**

https://owasp.org/www-project-top-10-insider-threats/

Motivation

Social Engineering Cyberattacken um 270% gestiegen (in 2021)

(Quelle: SLASHNEXT)

Motivation

90% von Data Breaches sind initial auf Phishing zurückzuführen (in 2021)

(Quelle: CISA)

Chishing

Herausgeber et al. (Hrsg.): Sicherheit,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 1

Business Chat ist verwirrt. Es hat sich vor Verwirrung selbst verletzt! - Chishing

Moritz Gruber, Christian Höfig, Matteo Große-Kampmann [1], Tobias Urban, Norbert Pohlmann[2]

Abstract: In dieser Arbeit wird eine ganzheitliche Bedrohung für Business-Chat-Anwendungen aufgezeigt und bewertet: *Chishing* – Phishing über Business-Chats. Die Bedrohung hat ihren Ursprung in den Anfängen der heutigen vernetzten Welt und das zugrunde liegende Problem wird als *Spoofing* in seiner einfachsten Form bezeichnet. In vier von sechs Business-Chat-Tools, die in dieser Arbeit analysiert werden, ist es möglich, Anzeigenamen, Profilbilder und weitere persönliche Informationen erfolgreich zu fälschen. Dies stellt eine Bedrohung für Unternehmen dar, da es Insider-Bedrohungen Vorschub leistet und unter Umständen auch externen Entitäten dazu einlädt, sich als interne Mitarbeiterin auszugeben.

Keywords: Phishing; Chishing; Social Engineering; Business Chats

Screenshot vom Chishing-Paper

Link zum Paper

Relevanz von Chishing

- Neue Angriffsvektoren fördern Social Engineering Angriffe.
- Besonders Unternehmen stehen im Fokus.
- Business Chats haben sich stark etabliert
- Chishing ist eine neue Ausprägung von Phishing

Chishing - Was ist das?

(Business) Chat + Phishing = **Chishing**

Identitätsübernahme bzw. Spoofing einer fremden Identität.

Im Kontext von Chishing:
Übernahme von Identitäten in Business Chats

Chishing - Welche Business Chats wurden getestet?

Microsoft Teams

Mattermost

Element

Slack

Google Chat

WebEx Teams

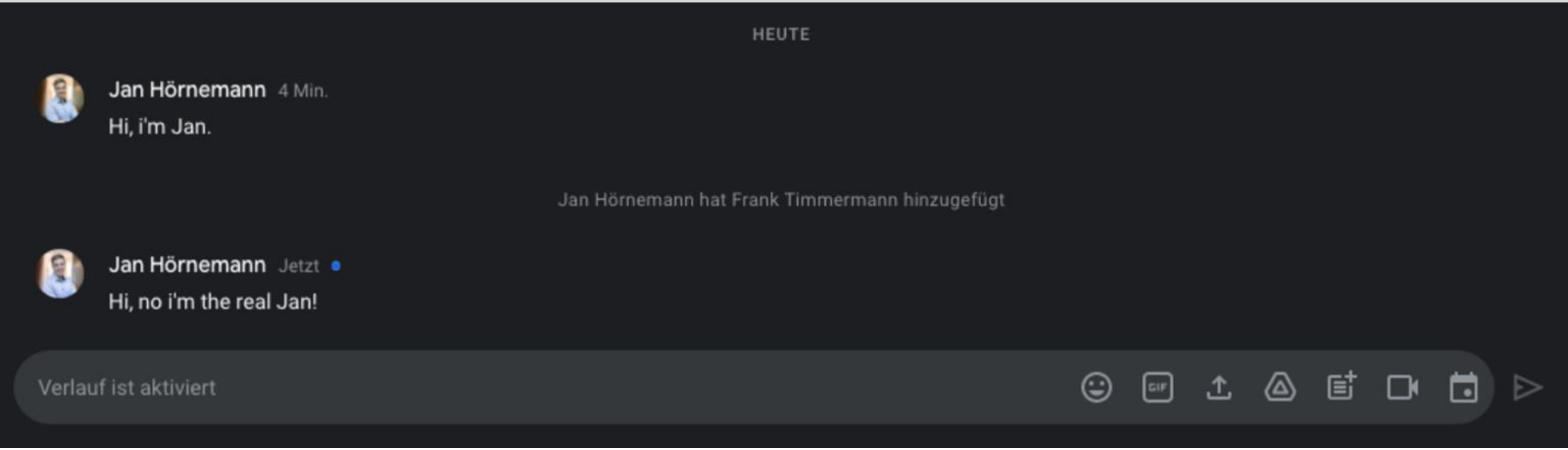
Chishing - Was wurde getestet?

Lässt sich das Profilbild ändern?

Lässt sich der Benutzername ändern?

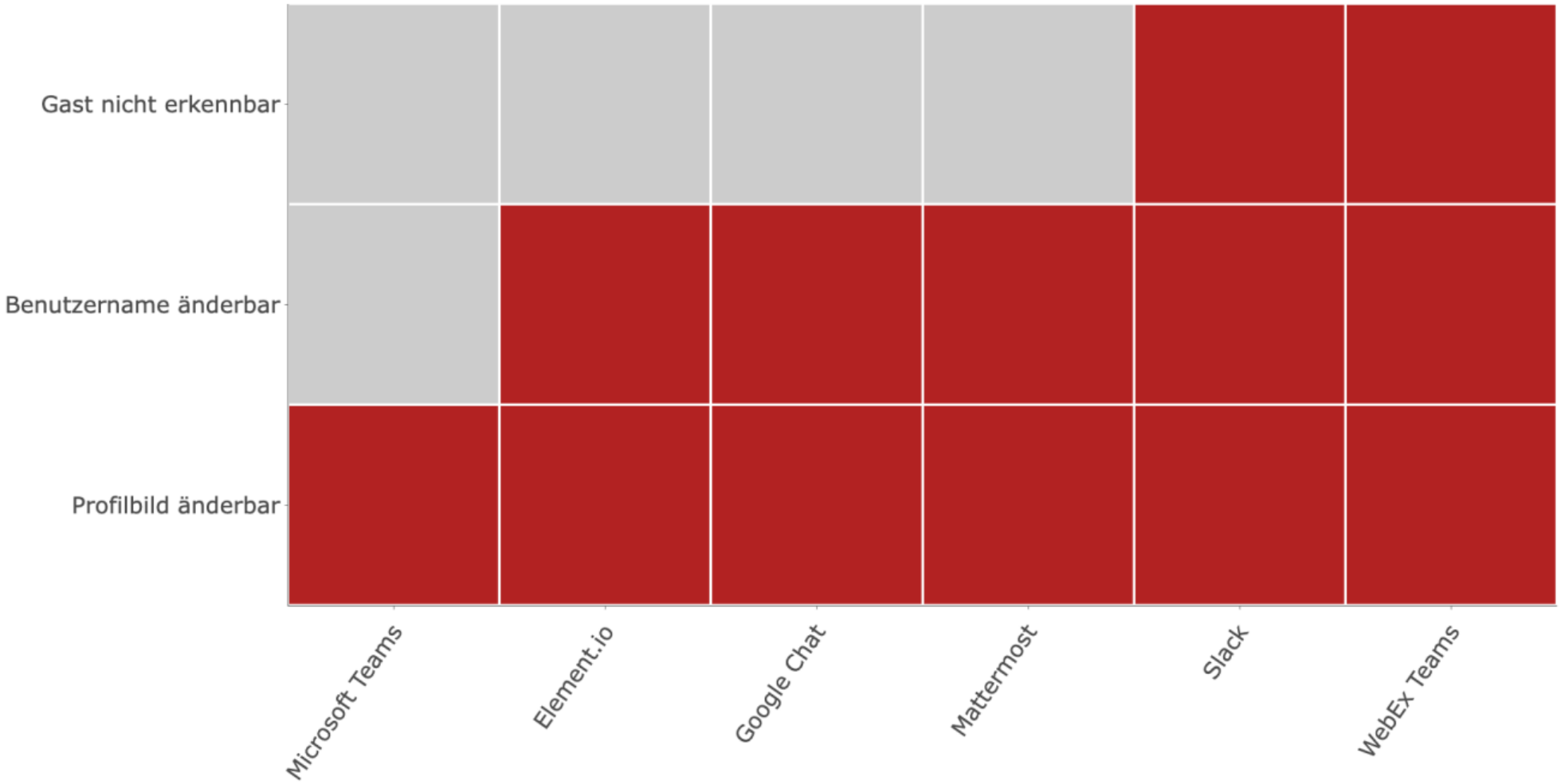
Ist der Benutzer als Gast erkennbar?

Chishing - Beispiele



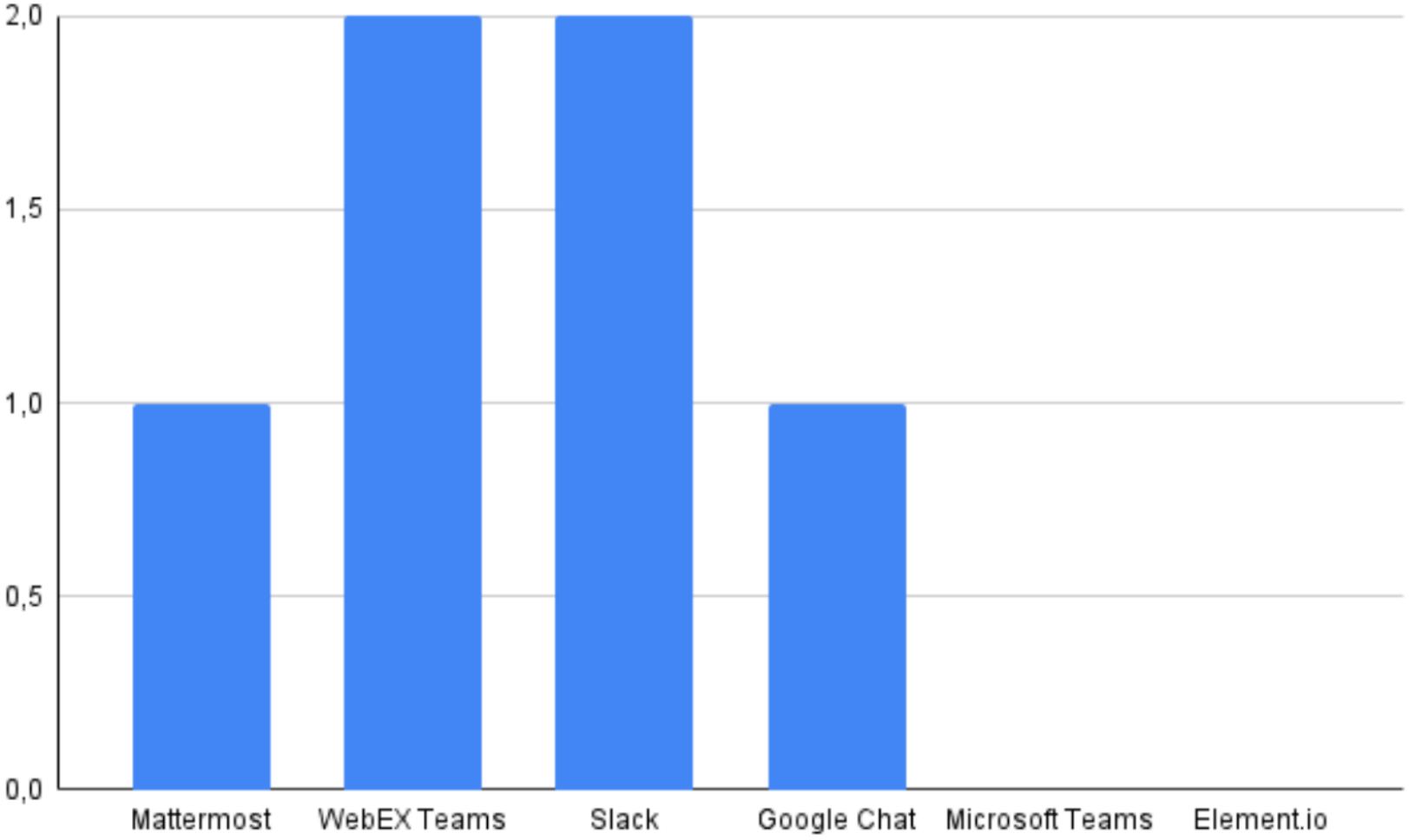
Chishing in Google Chat

Chishing - Was sind die Ergebnisse?



Ergebnisse der Analyse der Business Chats in Bezug auf Chishing

Chishing - Was sind die Ergebnisse?



Anzahl der benötigten Klicks um Identität zuprüfen

Benötigte Anzahl der Klicks um tatsächliche Identität festzustellen

Je höher die Anzahl, desto aufwändiger und unwahrscheinlicher die Feststellung

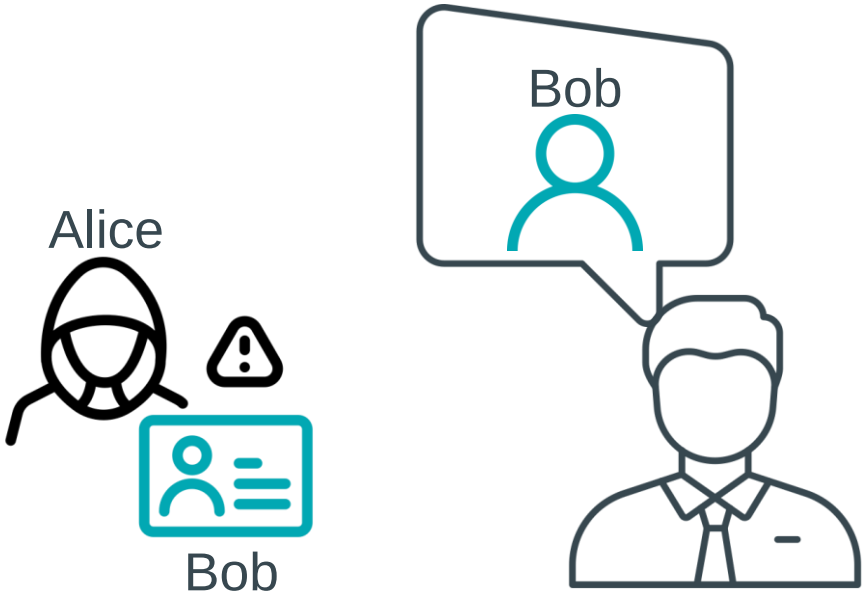
Chishing - Warum ist Chishing relevant?

Unternehmen sind im besonderen Fokus von APTs (Advanced Persistent Threat)

Social Engineering Cyberattacken um 270% gestiegen
(in 2021)

90% von Data Breaches sind initial auf Phishing zurückzuführen
(in 2021)

Social Engineering



Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen.

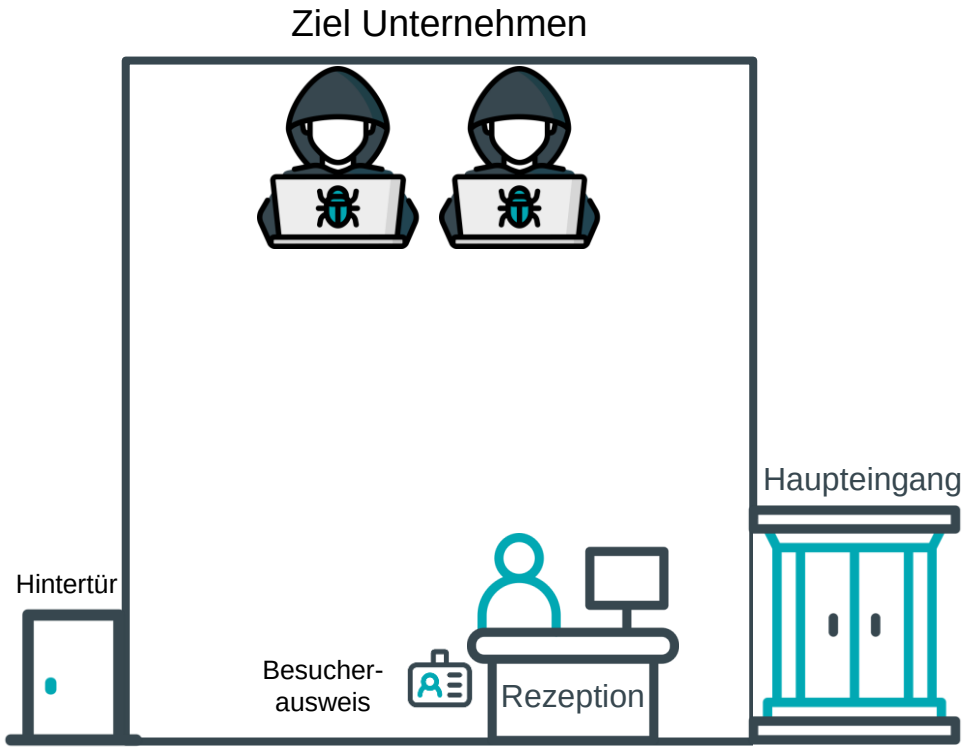
“Social Engineering nutzt Einfluss und Überzeugung, um Leuten glaubhaft zu machen, dass der Social Engineer jemand ist, der er nicht ist.”

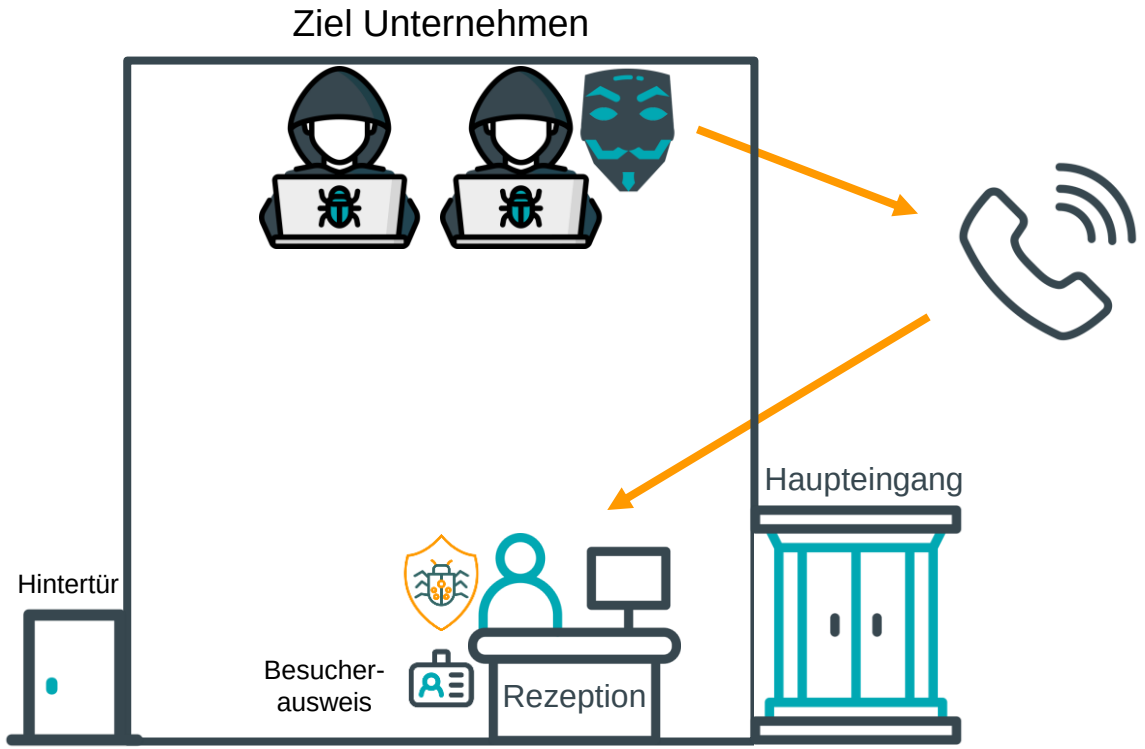
- Kevin Mitnick

Social Engineering - Tailes from a Social Engineer

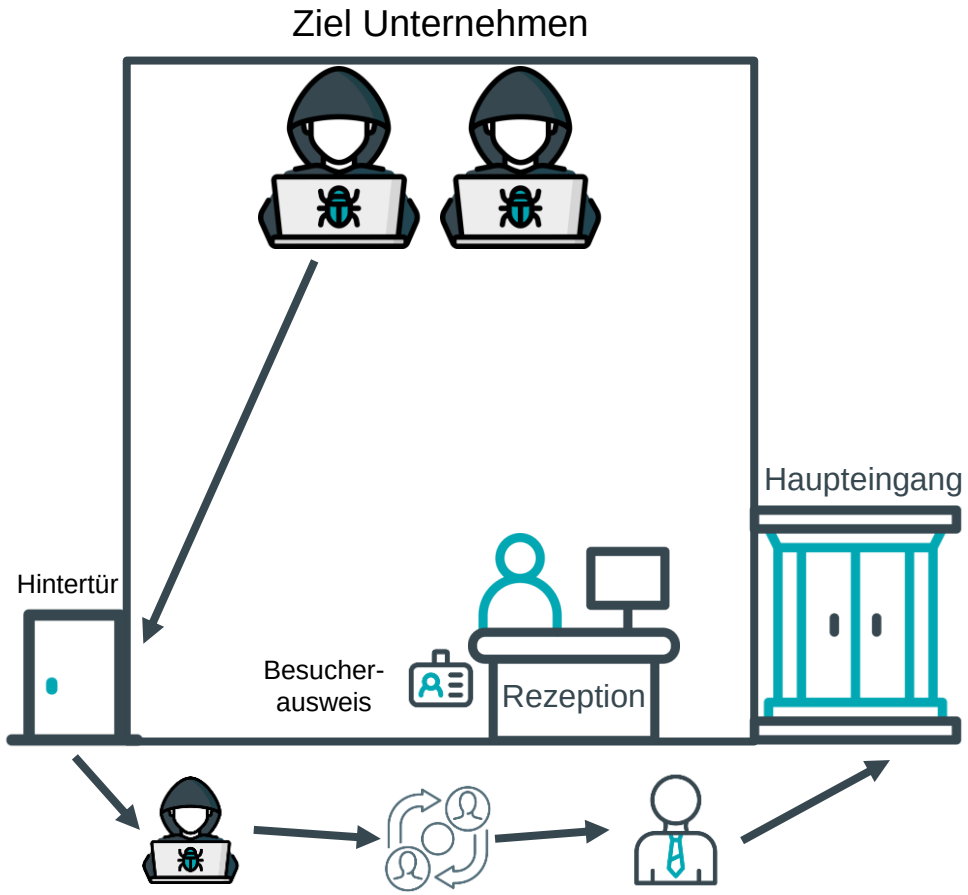
Tailes from a
Social Engineer

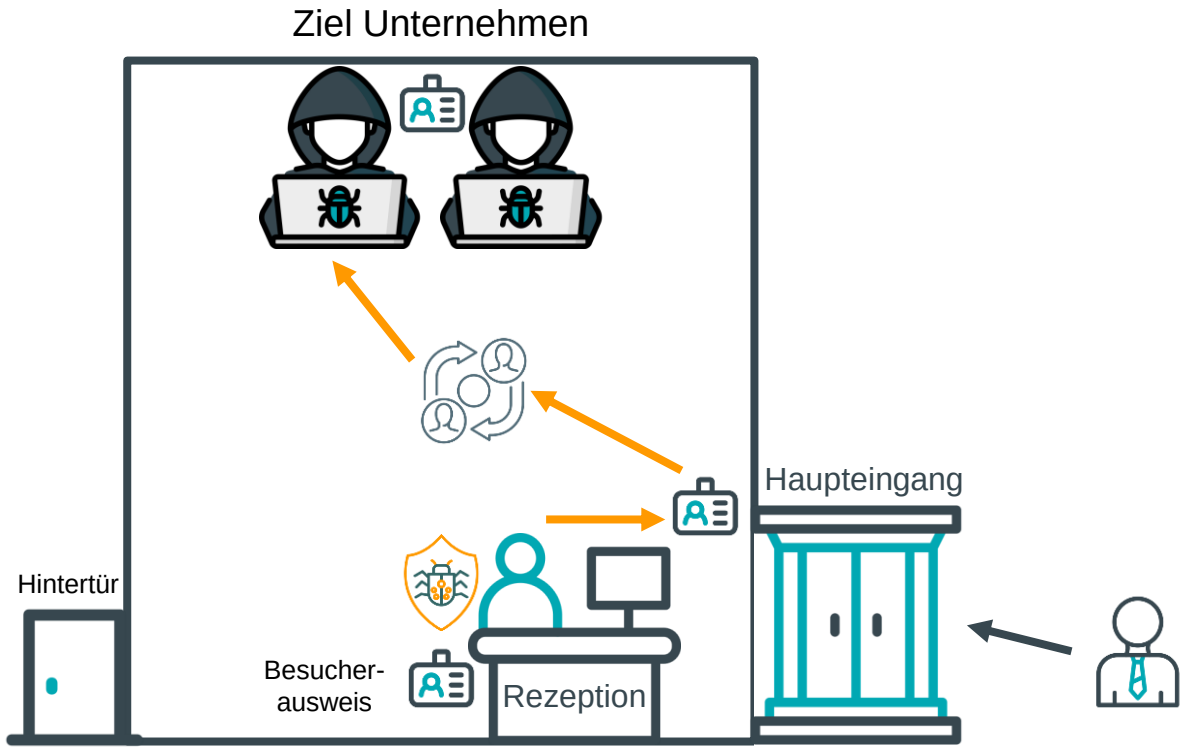
Beschaffung eines validen Besucherausweises



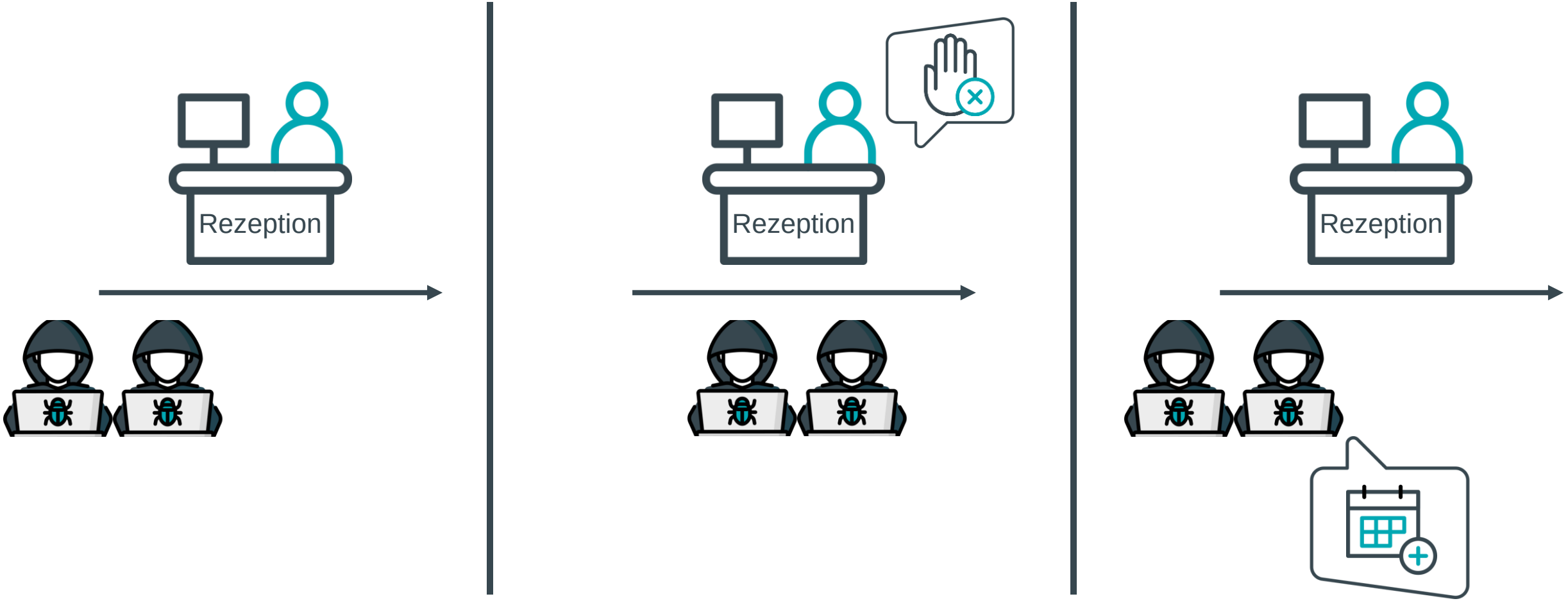


Beschaffung eines validen Besucherausweises

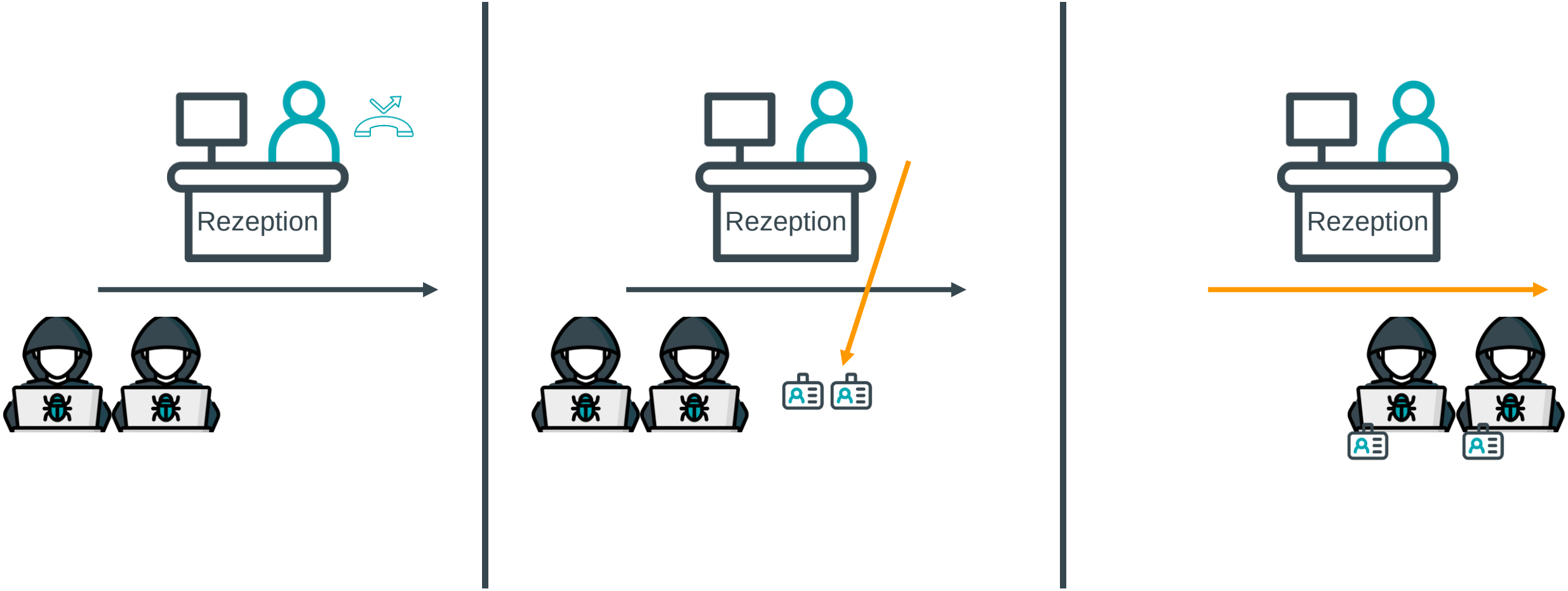




“Validen” Zutritt zum Gebäude und Geschäftsführerbüro verschafft

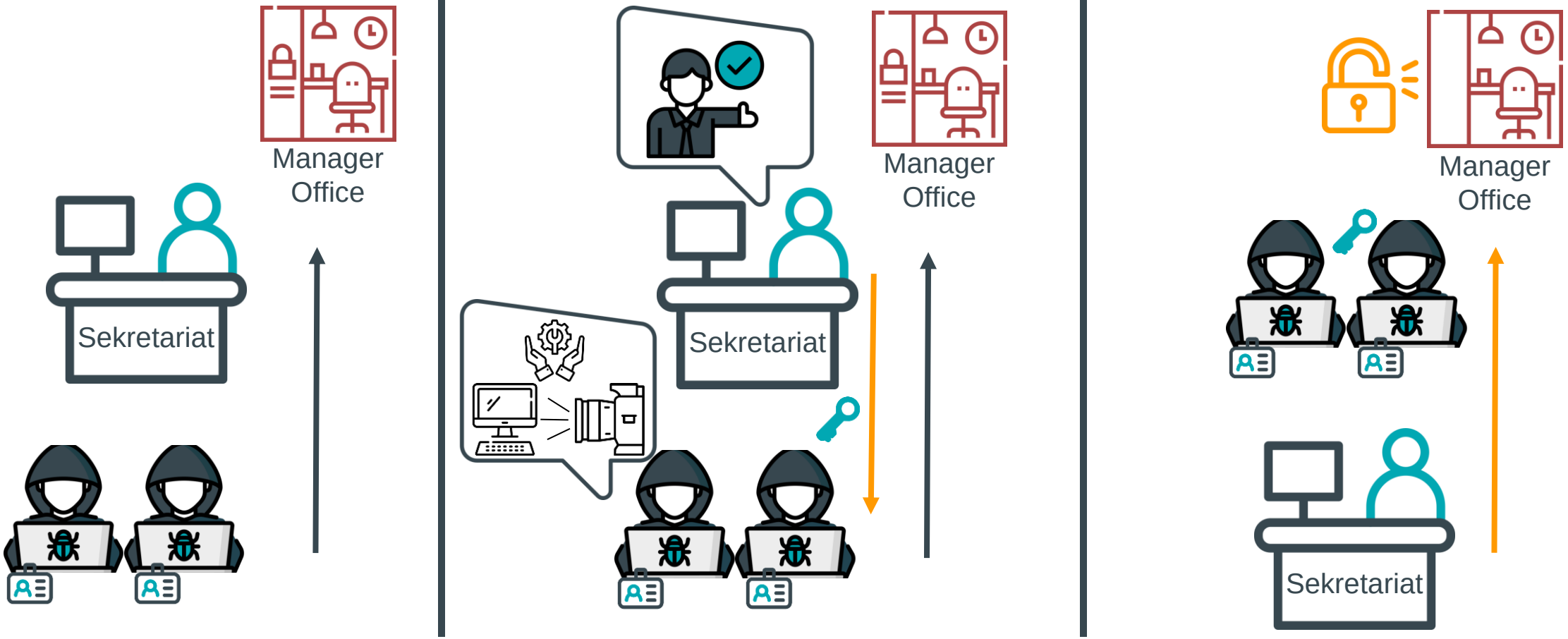


“Validen” Zutritt zum Gebäude und Geschäftsführerbüro verschafft



Social Engineering - Tailes from a Social Engineer - #2 Story

“Validen” Zutritt zum Gebäude und Geschäftsführerbüro verschafft



Relevanz und Bedeutung von Social Engineering

Unternehmen sind im besonderen Fokus von APTs (Advanced Persistent Threat)

Social Engineering Cyberattacken um 270% gestiegen
(in 2021)

Link zum Comic

Relevanz und Bedeutung von Social Engineering

Vielen Dank

Rückfragen?

Munscheidstrasse 14
Im Wissenschaftspark
45886 Gelsenkirchen

49 (0) 209 8830 6760

info@aware7.de

LinkedIn

Bei Rückfragen gerne jederzeit eine Nachricht schreiben:

nick@aware7.de

Nick Lorenz
Information- / IT-Security Consultant:
Penetrationstester und Referent / Dozent bei...

https://www.linkedin.com/in/nicklorenz

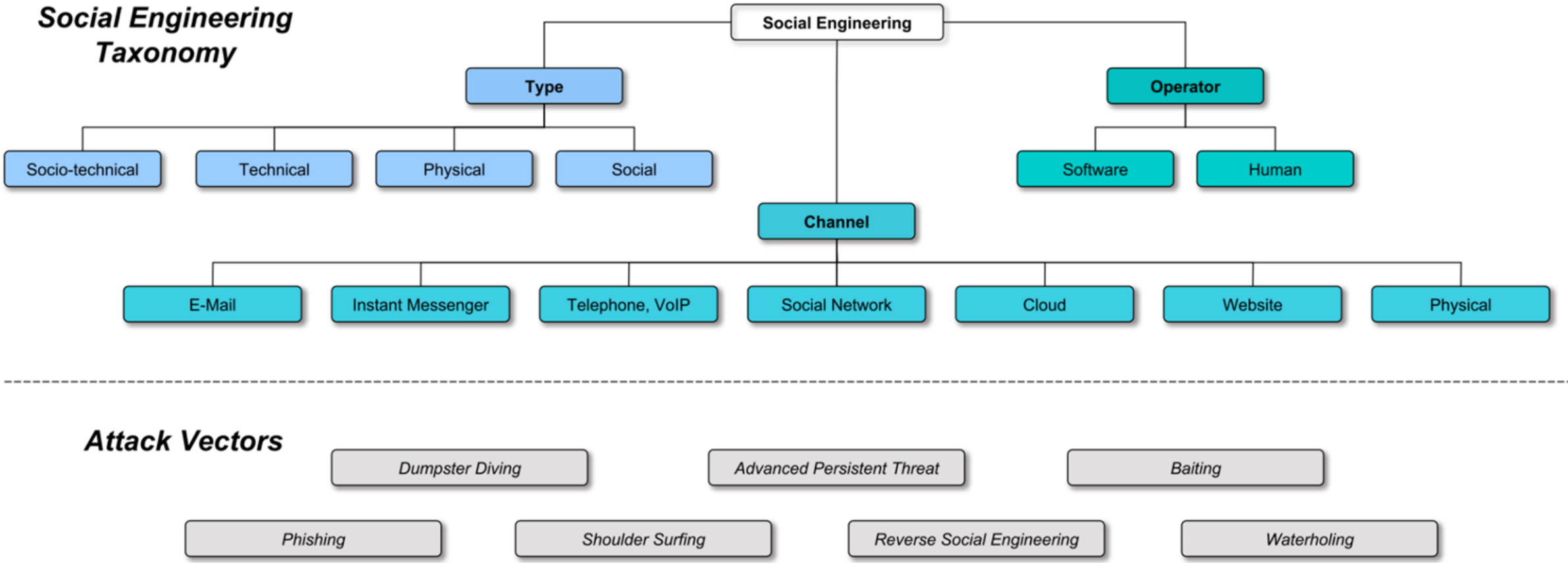


Fig. 1 – Overview of our classification of attack characteristics and attack scenarios.

Link zum Paper