Der Mensch als das stärkste Glied der Sicherheitskette

David Scribane – IT-Forum Fast Lane Berlin, 1.9.2022

Wenn man sich Informationssicherheitsvorfälle der letzten Jahre anschaut, dann sind viele darauf zurückzuführen, dass Mitarbeitende die grundsätzlichsten Regeln für den Schutz von Informationen nicht eingehalten haben.

Ingolstadt/Berlin

Massiver Hackerangriff auf Hunderte Politiker und Prominente

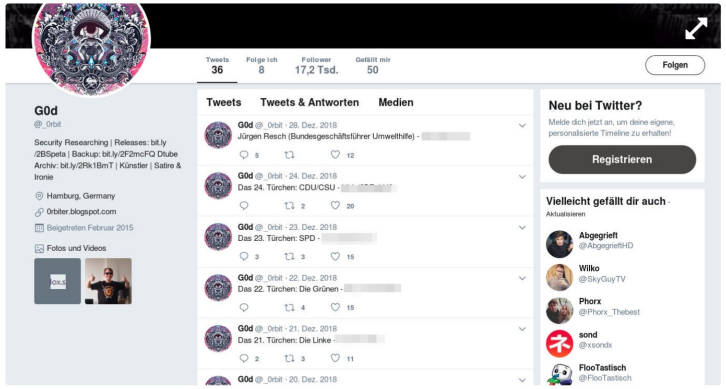
Twitter-Account mittlerweile gesperrt - Auch Ingolstadts MdB Reinhard Brandl betroffen

04.01.2019 | Stand 02.12.2020, 14:55 Uhr

AAA

Horst Richter

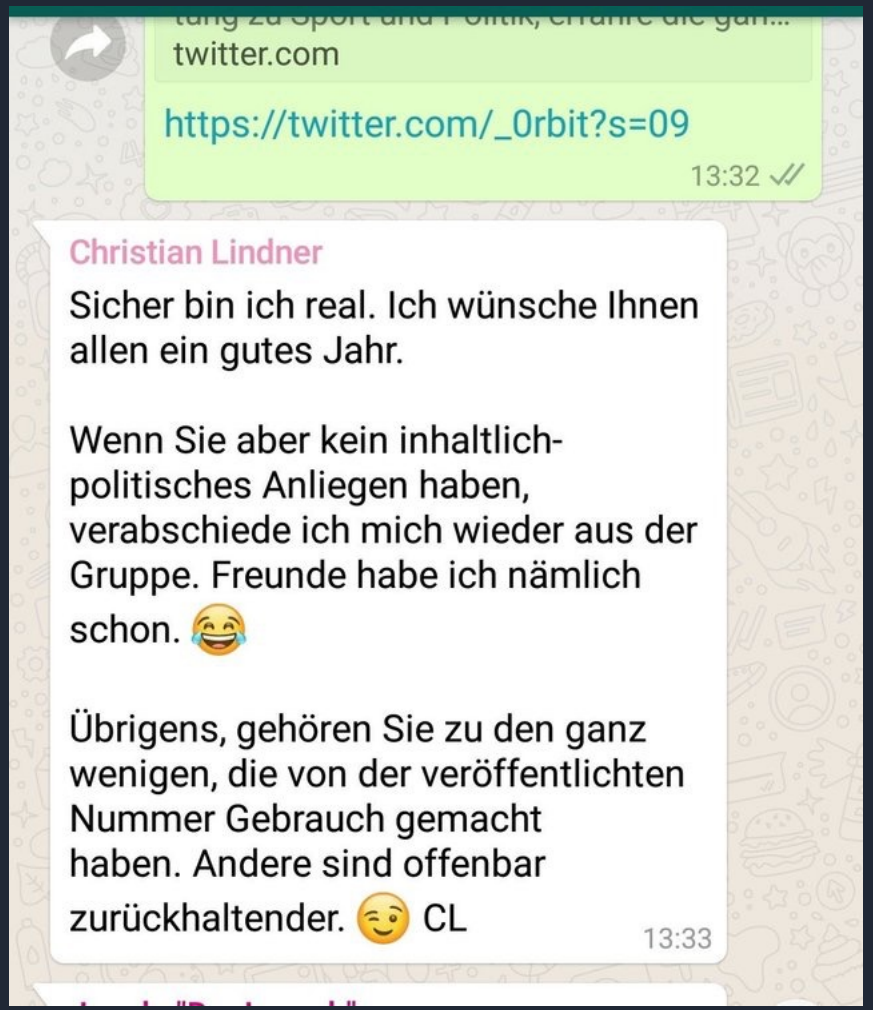
Regionalreporter



Mit Posts von diesem Twitter´-Profil wurden die Daten veröffentlicht. –Foto: Horst Richter

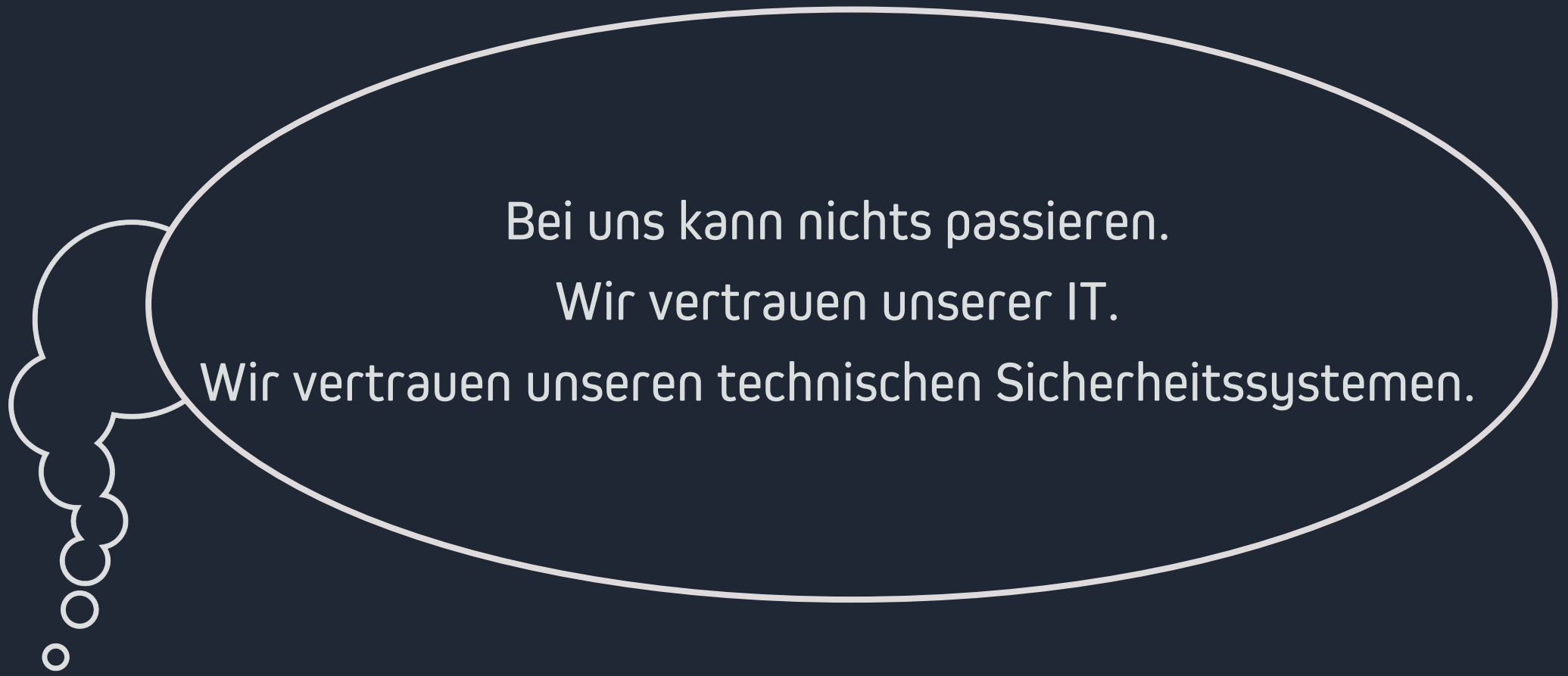
Berlin/München (DK) Ein Hackerangriff ungeahnten Ausmaßes erschreckt nicht nur Politiker, Prominente und andere Geschädigte. Über ein Twitter-Konto waren seit Dezember höchstpersönliche Daten von einigen hundert Bundestagsabgeordneten und Parteimitgliedern der CDU/CSU, SPD, Grüne, Linken und der FDP, aber auch von Satirikern und anderen veröffentlicht worden.

Aus der Region Ingolstadt traf es unter anderem den Ingolstädter CSU-MdB Reinhard Brandl, nach ersten Erkenntnissen allerdings nur mit der Bekanntgabe der Mobilfunknummer. MdB Alois Karl, zuständig für Teile unseres östlichen Verbreitungsgebiets, steht ebenfalls auf der Leak-Liste. Wer hinter dem bislang wohl größten Datenabgriff dieser Art in Deutschland steckt, ist noch offen. Zumindest das Regierungsnetz in Berlin scheint nach den ersten Erkenntnissen nicht betroffen oder die Quelle der gestohlenen Informationen zu sein. Nicht alle kamen so glimpflich weg wie Reinhard Brandl oder beispielsweise auch Bayerns



Der Mensch als das stärkste Glied der Sicherheitskette

Häufige Annahme



Wie Virenscanner funktionieren

Wie Virenscanner auch funktionieren

Faktoren für den Schutz von Informationen

Achtsame Mitarbeitende sind genauso wichtig wie ein aktueller Virenscanner.

Maßnahmen

Inhaltsfilter Blacklisting Schwachstellenmanagement

Bauliche Maßnahmen E-Mail-Inhaltsverschlüsselung geplant

Anti-SPAM-Filter Mobile Device Management **Big Data-Klassifizierung**

Monitoring Cloud-Richtlinien Desktop-Virtualisierung **Virenscanner** Follow-Me-Print

Redundante Infrastruktur Zugriffsberechtigungen Mehrere Rechenzentren Dateityp-Sperrung

Vermeidung lokaler Datenspeicherung **USB-Security** Transportverschlüsselung

Patchmanagement Servervirtualisierung Alerting Anti-Malware-Filter

Zertifizierte Dienstleister **Mehrstufige Firewallsysteme** Werbeblocker

Virtual Private Network Backup- und Recovery

Festplattenverschlüsselung

Maßnahmen

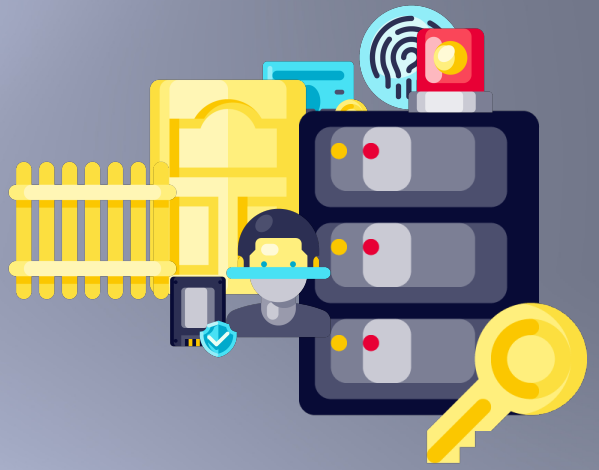
Business-Continuity Management
Business Impact Analysen
IT-Security-Strategie
Zutrittskonzepte
Inhaltsfilter
Blacklisting
Schwachstellenmanagement
Arbeitsgemeinschaften
Beschäftigtenrichtlinien
Bauliche Maßnahmen
E-Mail-Inhaltsverschlüsselung geplant
Social-Media-Guidelines
Notfallmanagement
Anti-SPAM-Filter
Mobile Device Management
Big Data-Klassifizierung
Unterweisungen
Monitoring
Cloud-Richtlinien
Desktop-Virtualisierung
Virenscanner
Follow-Me-Print
Offline-Dokus
Audits
Redundante Infrastruktur
Zugriffsberechtigungen
Mehrere Rechenzentren
Dateityp-Sperrung
Zertifizierungen
Vermeidung lokaler Datenspeicherung
USB-Security
Transportverschlüsselung
Notfallhandbuch
IT-Risikomanagement
Patchmanagement
Servervirtualisierung
Alerting
Anti-Malware-Filter
Krisenstab
Netiquette
Zertifizierte Dienstleister
Mehrstufige Firewallsysteme
Werbeblocker
Prozessanpassungen
Schutzbedarfsfeststellungen
Virtual Private Network
Backup- und Recovery
E-Mail-Richtlinien
Informationssicherheitsmanagement
Festplattenverschlüsselung
Sicherheitskonzepte
Beschaffungspolicies
Katastrophensimulationen
Informationssicherheitsbeauftragte
Onboarding-Plans

Maßnahmen


Business-Continuity Management
Business Impact Analysen
IT-Security-Strategie
Zutrittskonzepte
Inhaltsfilter
Blacklisting
Schwachstellenmanagement
Arbeitsgemeinschaften
Beschäftigtenrichtlinien
Bauliche Maßnahmen
E-Mail-Inhaltsverschlüsselung geplant
Social-Media-Guidelines
Notfallmanagement
Anti-SPAM-Filter
Mobile Device Management
Big Data-Klassifizierung
Unterweisungen
MonitoringCloud-Richtlinien
Desktop-Virtualisierung
Virenscanner
Follow-Me-Print
Offline-Dokus
Audits
Redundante Infrastruktur
Zugriffsberechtigungen
Mehrere Rechenzentren
Dateityp-Sperrung
Zertifizierungen
Vermeidung lokaler Datenspeicherung
USB-Security
Transportverschlüsselung
Notfallhandbuch
IT-Risikomanagement
Patchmanagement
Servervirtualisierung
Alerting
Anti-Malware-Filter
Krisenstab
Netiquette
Zertifizierte Dienstleister
Mehrstufige Firewallsysteme
Werbeblocker
Prozessanpassungen
Schutzbedarfsfeststellungen
Virtual Private Network
Backup- und Recovery
E-Mail-Richtlinien
Informationssicherheitsmanagement
Festplattenverschlüsselung
Sicherheitskonzepte
Beschaffungspolicies
Katastrophensimulationen
Informationssicherheitsbeauftragte
Onboarding-Plans

Social Engineering

IT-Sicherheitsthemen



SOCIAL ENGINEERING

Menschen werden dazu gebracht, Dinge zu tun, die sie nicht tun möchten, ohne dass sie es merken, dass sie es tun.

Menschliche Eigenschaften

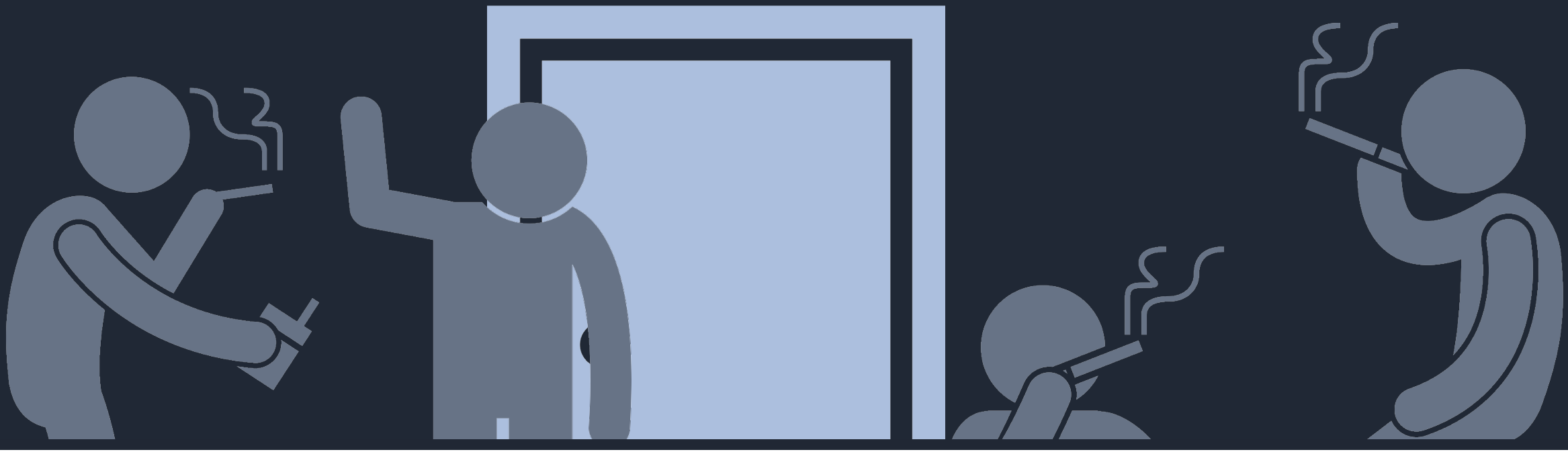
- Hilfsbereitschaft
- Neugier
- Reziprozität
- Autoritätshörigkeit
- Lob/Anerkennung

- Angst
- Harmoniebedürfnis
- Habgier
- Vertrauen
- Stressresilienz

Menschliche Eigenschaften

Hilfsbereitschaft

Hilfsbereitschaft / Höflichkeit

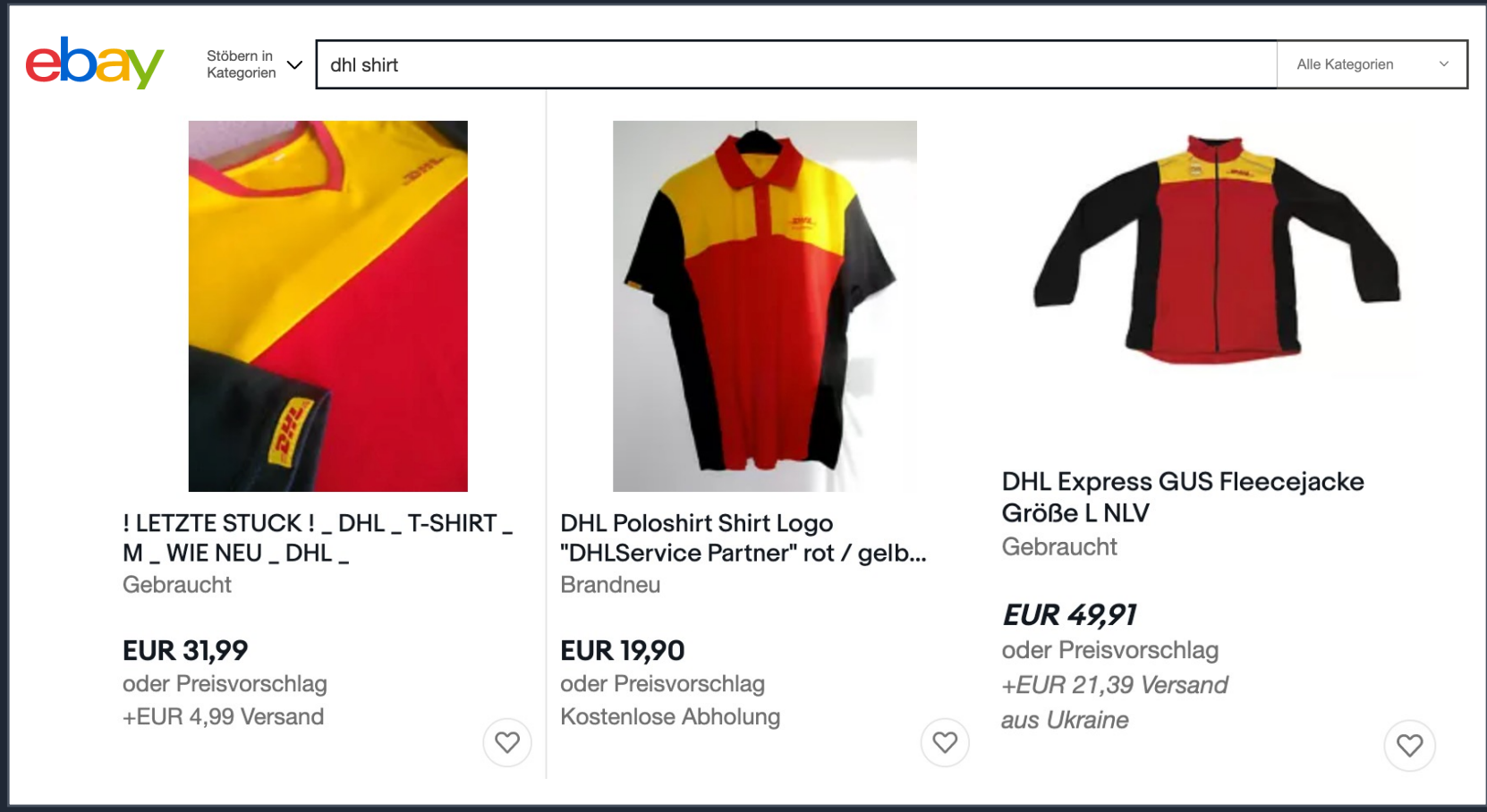


Rauchen kann Ihre Informationssicherheit gefährden.

Hilfsbereitschaft / Höflichkeit

Man nehme:

- Drei Pappkartons
- Ein Paketbotenshirt
- Einen Anzug
- Ein Außer-Betrieb-Schild



Menschliche Eigenschaften

Autoritätshörigkeit

Dumpster Diving

Hilfsbereitschaft

Reziprozität

Vertrauen

Reziprozität

Hilfsbereitschaft

Vertrauen

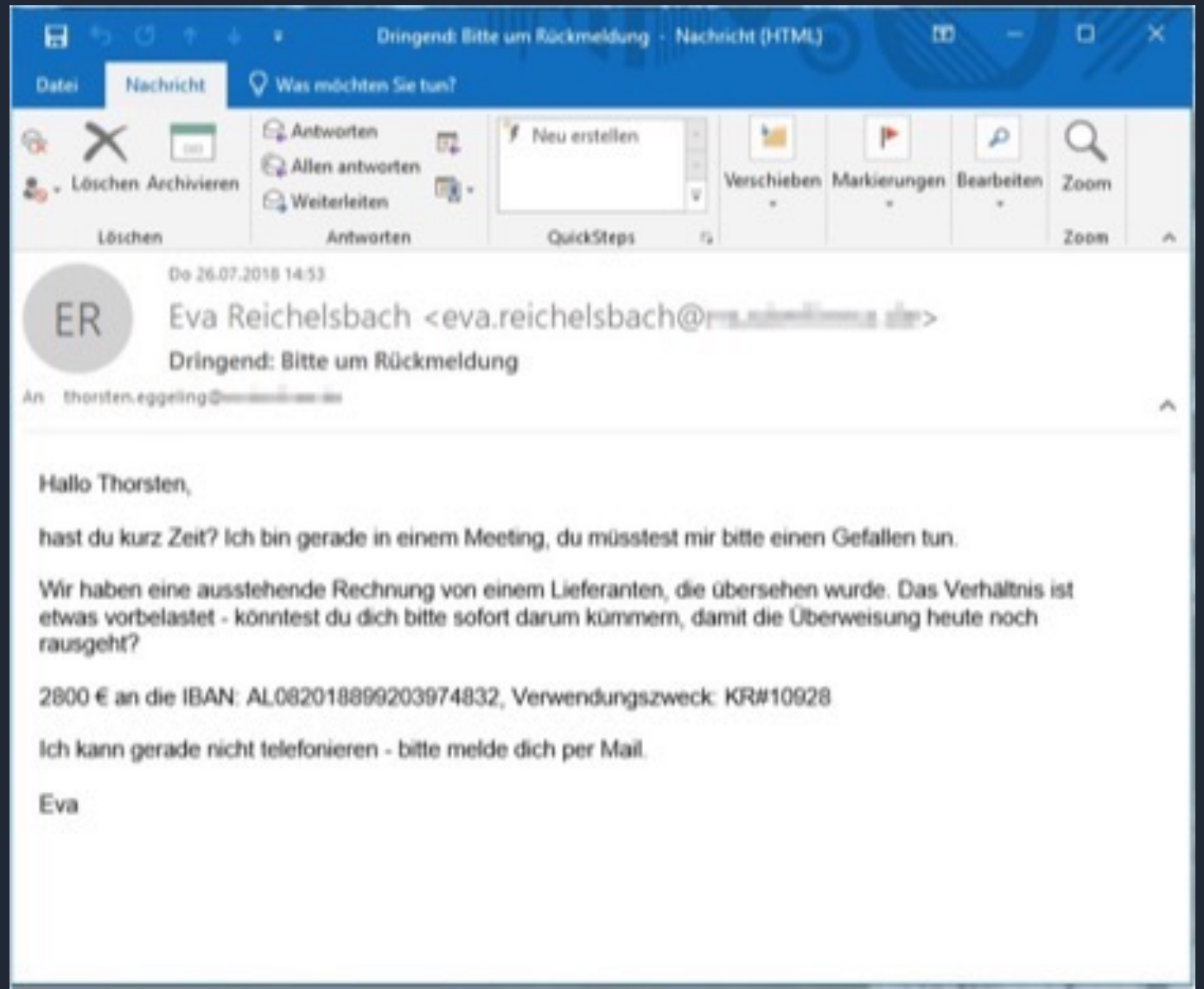
BEFRAGUNG

Stressresilienz

Lob/Anerkennung

Autoritätshörigkeit

Kontext ist König!



- Rückversicherung über anderes Medium (z.B. Telefon/ Teams/ Flur)
- Auch wenn der Absender dies nicht wünscht!
- Auch wenn der Absender nicht erreichbar ist.
- Auch wenn Zeitdruck aufgebaut wird.

Menschliche Eigenschaften

Stressresilienz

Menschliche Eigenschaften

Stressresilienz

Informationsgewinnung

Vorlieben, Filme, Musik, Einkäufe, Bekanntschaften, Einstellungen, Wohnort, Ereignisse, Beruf, Lebensstationen, Fotos, Geburtstag etc.

Informationen machen Angriffe überzeugender

Neugier

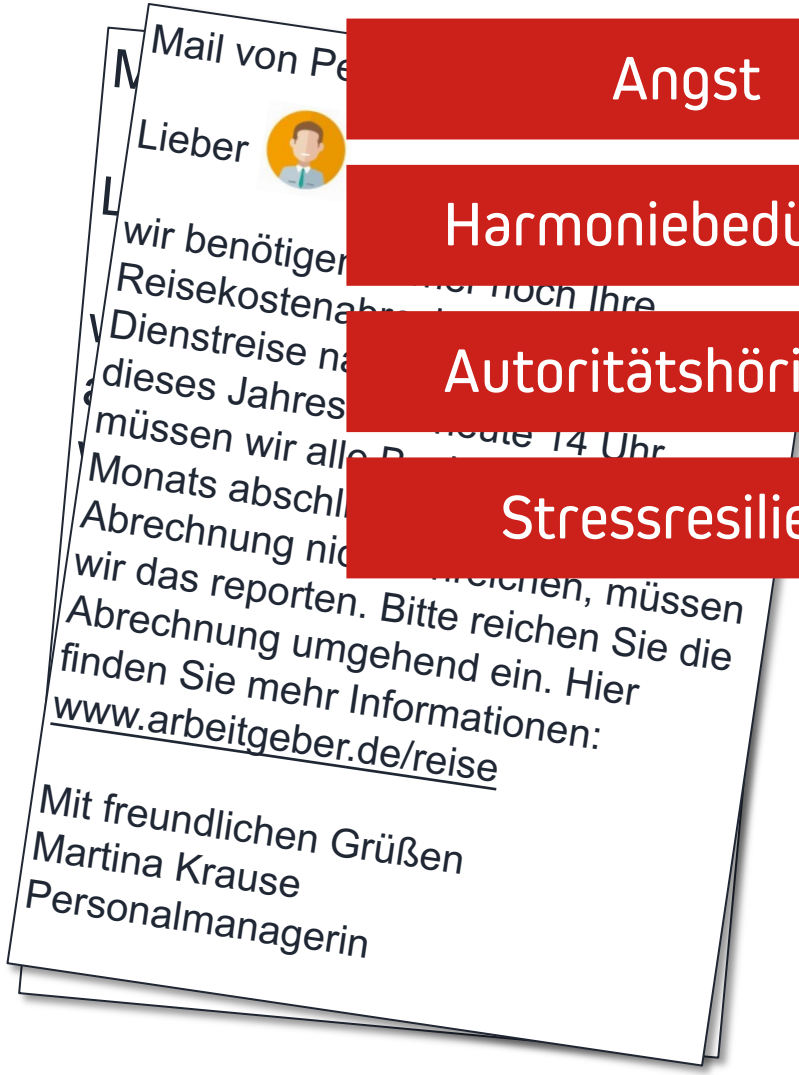
Mail von

Lieber ,

weißt Du noch letzte Woche, als wir im Konzert bei Pur waren? Schau mal, auf der Homepage vom Veranstalter sind wir gemeinsam zu sehen. Klick mal hier: http://www.pur.de/fotos

Beste Grüße,
Dein

Informationen machen Angriffe überzeugender



- Angst
- Harmoniebedürfnis
- Autoritätshörigkeit
- Stressresilienz

Ransomware / Crypto-Viren / Erpressungstrojaner

PDF-Dateien…

- …können (gefährliche) Inhalte aus dem Internet nachladen.
- …fordern dazu jedoch Ihr Einverständnis ein.
- Geben Sie das nicht, ist der Angriff erfolglos.

Office-Dateien…

- …können aktiven Schadcode ausführen – beispielsweise Viren installieren.
- …fordern dazu jedoch Ihr Einverständnis ein (Makros aktivieren, Inhalte aktivieren)
- Geben Sie das nicht, ist der Angriff erfolglos.

Ransomware / Crypto-Viren / Erpressungstrojaner

Daten sind im Grund noch vorhanden aber nicht zugreifbar.

Lösegeldforderung in einer Cryptowährung. Forderung an die Person/Organisation angepasst.

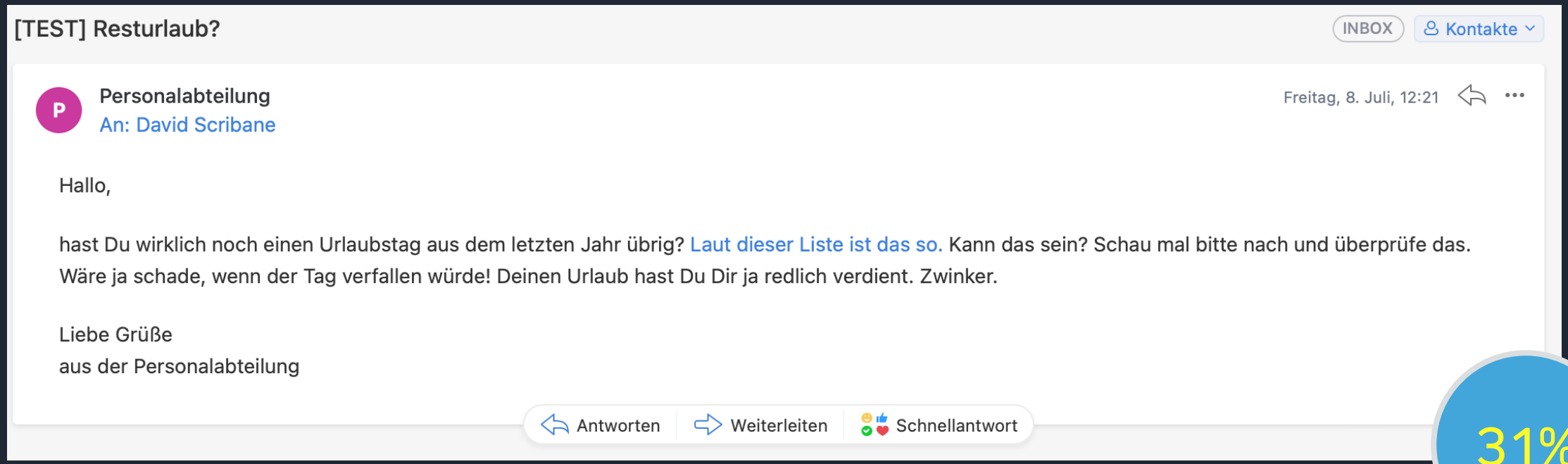
Virenvarianten:

- Kombination mit Abfluss von Informationen
- Mining von Cryptowährungen
- Besonders perfide: alternatives Infizieren von Freunden.

2019 - 2021: Emotet verursacht Milliardenschäden im DACH-Raum.

Seit 2020 verstärkt auch mit parallelem Abfluss der Daten.

Beispiel


[TEST] Resturlaub?
INBOX
Kontakte
P
Personalabteilung
An: David Scribane
Freitag, 8. Juli, 12:21
Hallo,
hast Du wirklich noch einen Urlaubstag aus dem letzten Jahr übrig? Laut dieser Liste ist das so. Kann das sein? Schau mal bitte nach und überprüfe das. Wäre ja schade, wenn der Tag verfallen würde! Deinen Urlaub hast Du Dir ja redlich verdient. Zwinker.
Liebe Grüße
aus der Personalabteilung
Antworten
Weiterleiten
Schnellantwort

31%

Großes Missverständnis

„Wer hat schon an mir Interesse?“

„Ich habe ja nichts mit Geschäftsgeheimnissen zu tun!“

„Wer soll etwas ausgerechnet von mir wollen?“

80% der Angriffe erfolgen nicht bei Geschäftsleitungen oder Personal mit Kontenzugang

- Informationsgewinnung für weitergehende Angriffe
- Informationsgewinnung für Wettbewerbsvorteile
- Informationsgewinnung für Veräußerung der Daten

Ansprachen per Mail, per Telefon oder direkt

Einen Social Engineering abzuwehren ist schwer.

Einen Social Engineering-Angriff zu erkennen ist jedoch noch schwerer.

„Ich hatte da ein komisches Gefühl.
Ich habe es aber bei Seite gelegt und gehandelt.“

Wichtige Tipps

Erkennung

Auf das Gefühl hören!

- Nicht in Handlungsdruck bringen lassen.
- Kurz innehalten!
- Handlungsoptionen bewerten
- Aus der Situation gehen (bspw. Rückruf anbieten)

Gesundes Misstrauen

Nicht von Äußerlichkeiten blenden lassen.

Visitenkarten sind kein Identitätsnachweis.

Den Druck Fremder nicht zum eigenen Druck machen lassen.

Abwehr

Einstudierte Aussagen nutzen, nicht auf lange Gespräche einlassen.

Konsequent bei einer Linie bleiben und an Vorgaben halten.

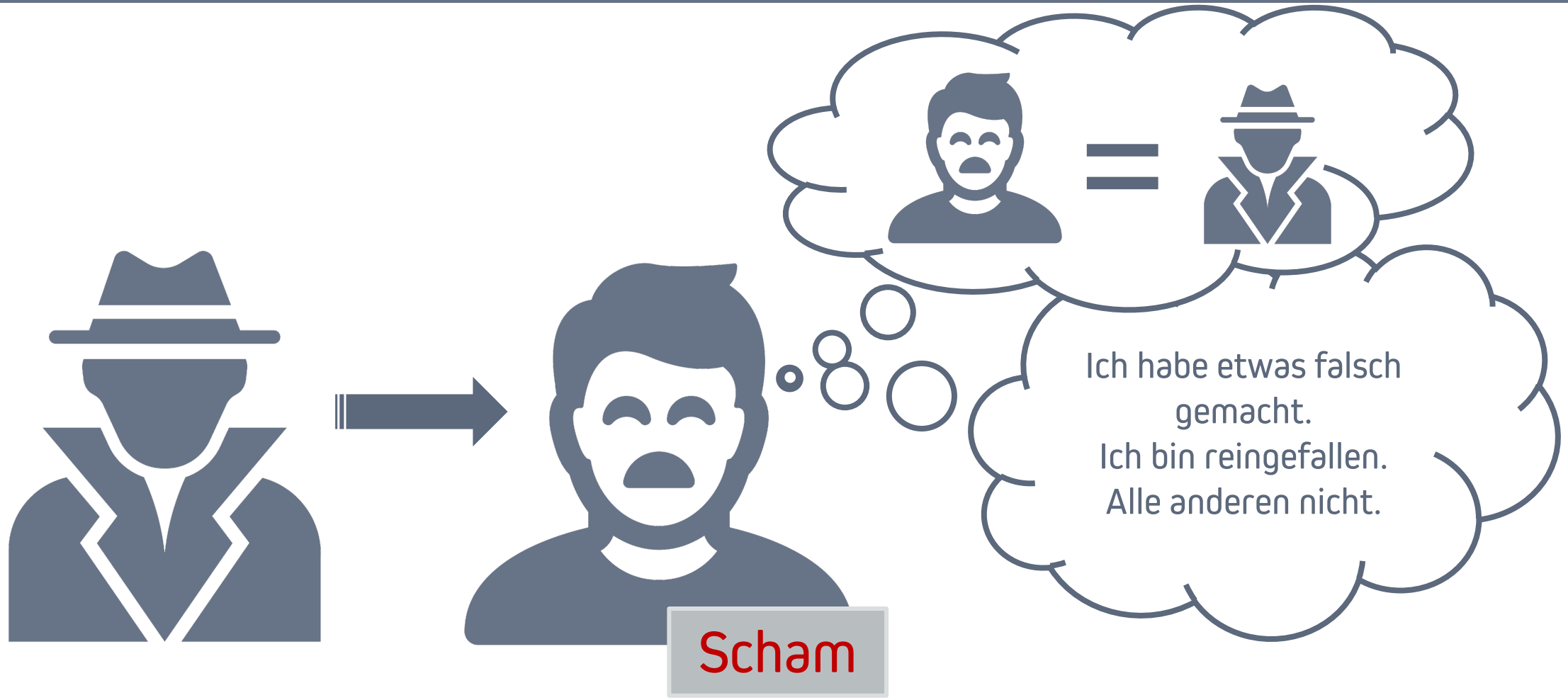
Anfragen und Gesprächsversuche nie persönlich nehmen.

Freundlich aber bestimmt bleiben.

- «Ich kann das gut verstehen, Frau Müller…»
- «Es tut mir furchtbar leid, Frau Müller…»

Üben, üben, üben.

Täter und Opfer



Mehr Infos: <kes> Die Zeitschrift für Informations-Sicherheit / Ausgabe Februar 2018, Seite 6

Täter und Opfer

Täter
Mittäter
Schwachstelle

Opfer
wichtigster Zeuge
Aufklärer

Technik ist nicht die alleinige Lösung.

Wir müssen unsere Sinne schärfen.

Auch für neue Herausforderungen.

Sensibilität

Fotos

E-Mails

Anrufe

Wir müssen Awareness aufbauen.

Awareness ist kein Patch,
den man über Nacht in eine Organisation einspielt.

Kein Sprint sondern ein Triathlon

Was also tun?

Den Schutz von Informationen aus der IT-Ecke holen

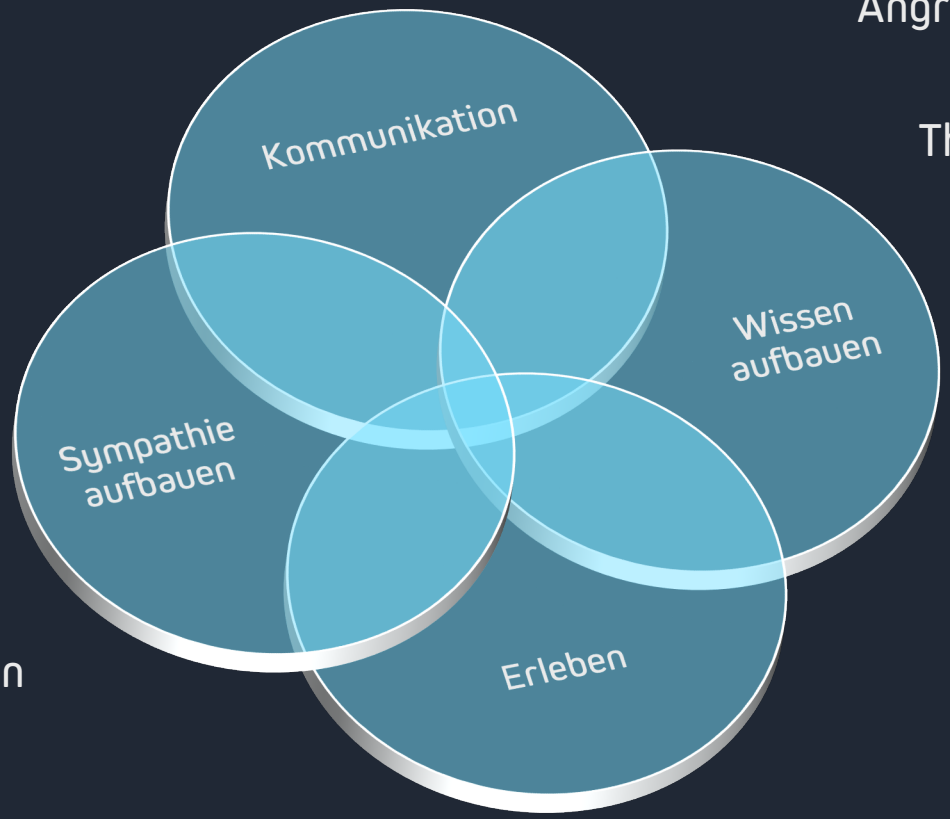
Überwinden der Fachsprache

Sinne entwickeln

Fehlerkultur stärken, positives Verhalten honorieren

Bezug zur Organisation herstellen

Phishing-Simulationen



Angriffe aufbereitet kommunizieren

Thema dauerhaft sichtbar halten

Kurzinterventionen

Kommunikative Erwartungshaltung berücksichtigen

Human Penetrationstests

Trainings und Workshops