(M)IT Sicherheit, geht mich das was an(!)?

IT-Sicherheit & die menschliche Firewall

Einstieg

Angriffspunkt Nr. 1:
Der Mensch

Praxistipps

Fragen?

für #zusammenwedemark Standortmarketing e.V.

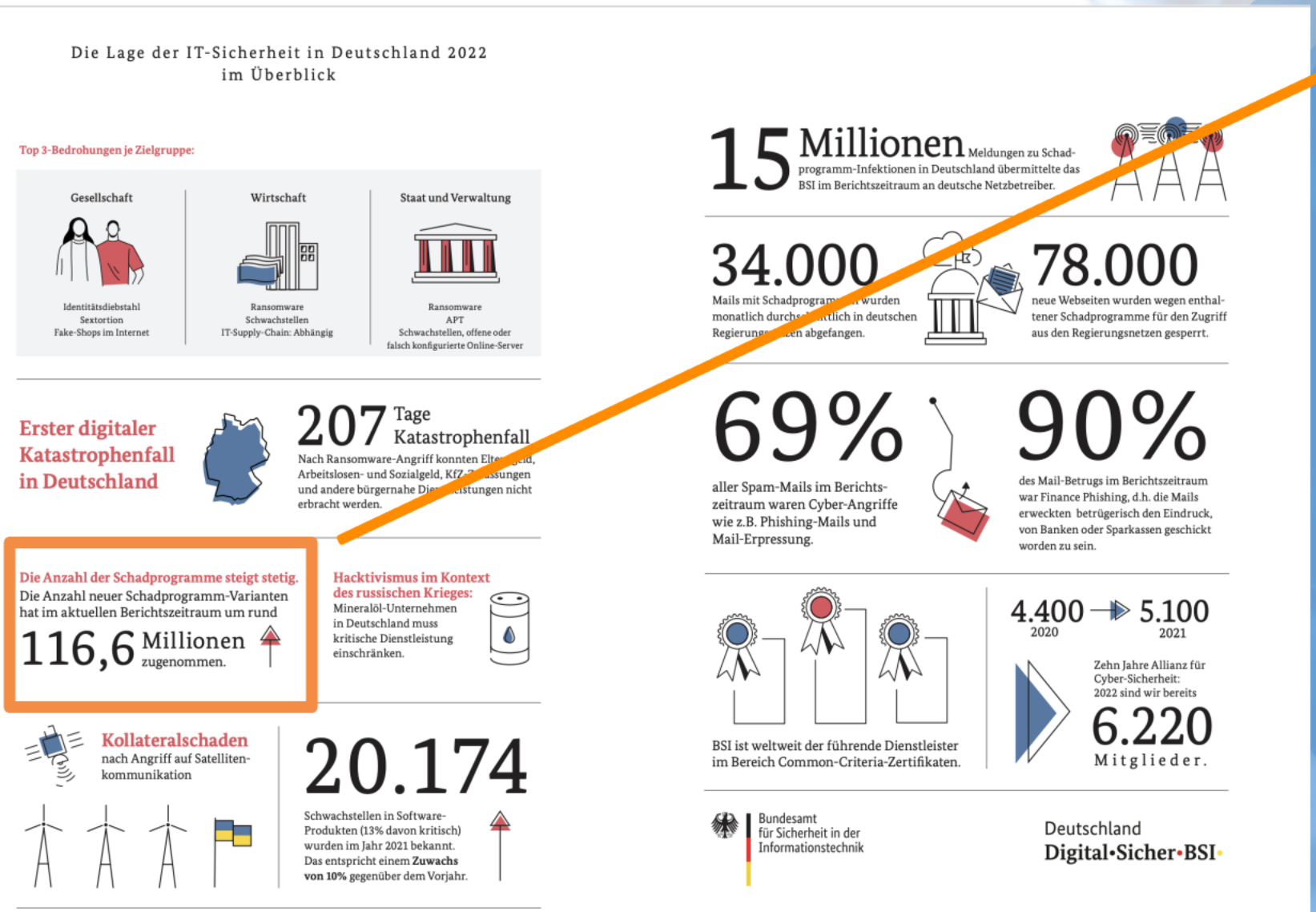
Warum
Sensibilisierung?

Ist unsere IT nicht
sicher genug?

Bedrohungslage

Bedrohungsarten

Grenzen technischer Hilfsmittel



Anzahl NEUER Schadprogramme

- Viren
- Trojaner
- Phishing
- etc.

Vorjahresvergleich

144 Mio. in 2021

> ca. **1 Mio. mehr pro Monat!**

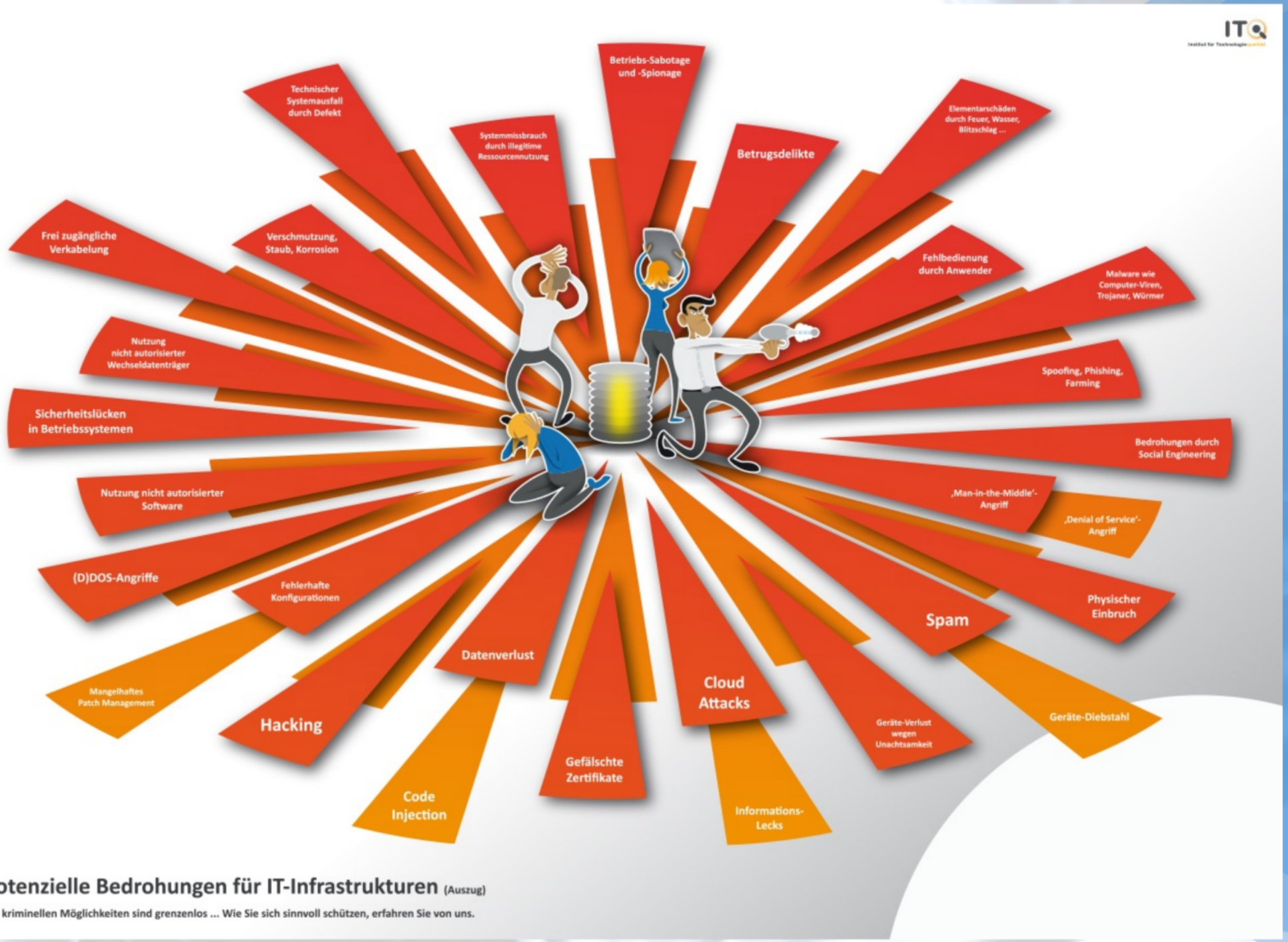
Warum
Sensibilisierung?

Ist unsere IT nicht
sicher genug?

Bedrohungslage

Bedrohungsarten

Grenzen technischer Hilfsmittel



Potenzielle Bedrohungen für IT-Infrastrukturen (Auszug)

Die kriminellen Möglichkeiten sind grenzenlos ... Wie Sie sich sinnvoll schützen, erfahren Sie von uns.

Warum
Sensibilisierung?

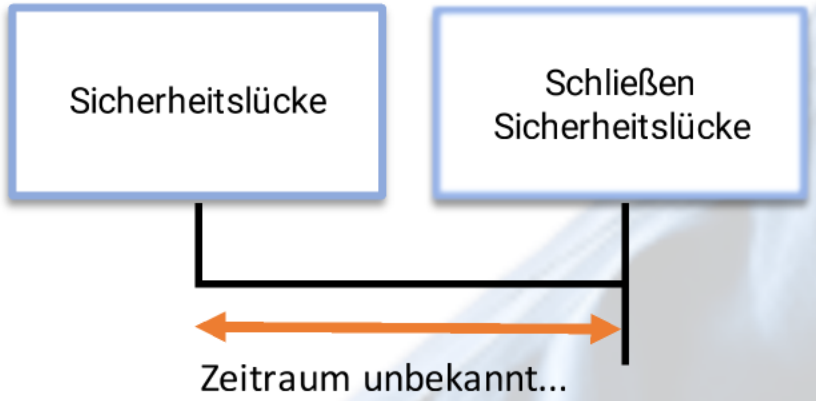
Ist unsere IT nicht
sicher genug?

Bedrohungslage

Bedrohungsarten

Grenzen technischer Hilfsmittel

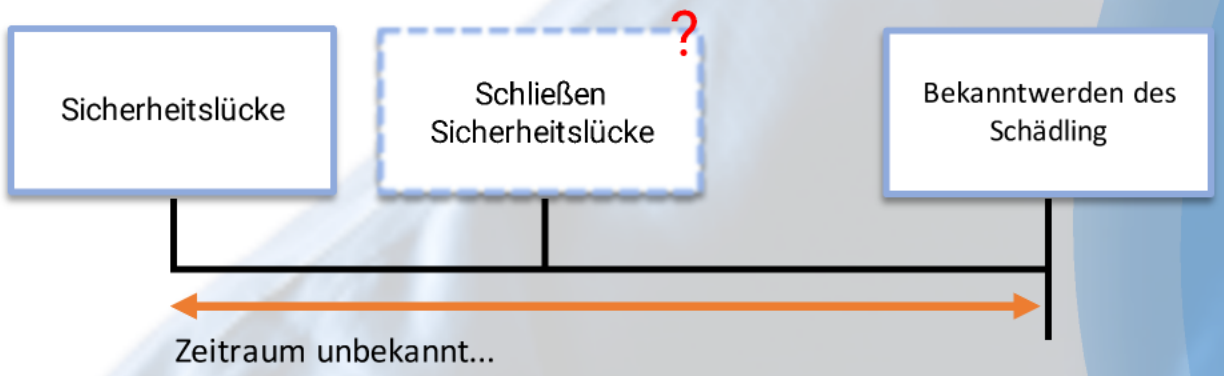
Typischer Verlauf eines Virenbefalls



- "Alle" IT-Systeme haben Sicherheitslücken
- Aufspüren von Sicherheitslücken ist Geschäftsmodell
- Schließen von Sicherheitslücken über Hersteller-Updates (Patches)
- Automatisierte Prozesse helfen!
- Nicht alle Sicherheitslücken werden frühzeitig erkannt!

Schädling wird bekannt

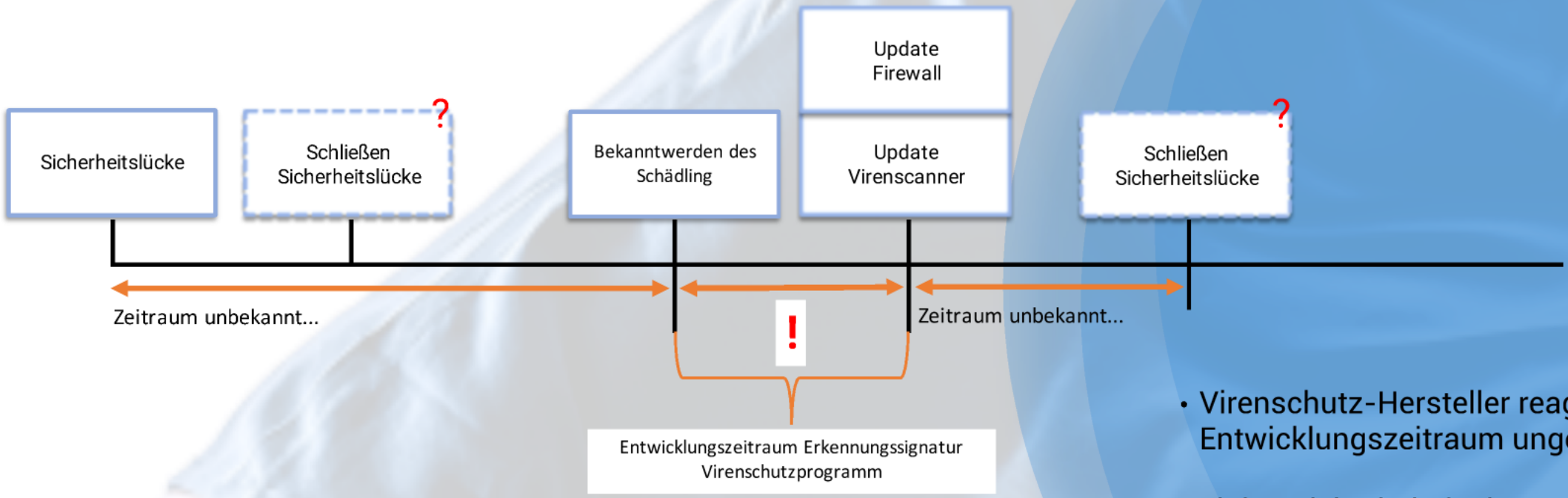
Typischer Verlauf eines Virenbefalls



- Nicht alle Sicherheitslücken werden frühzeitig erkannt!
- Nicht geschlossene Sicherheitslücken können angegriffen werden
- Ob und Wann ist ungewiss!

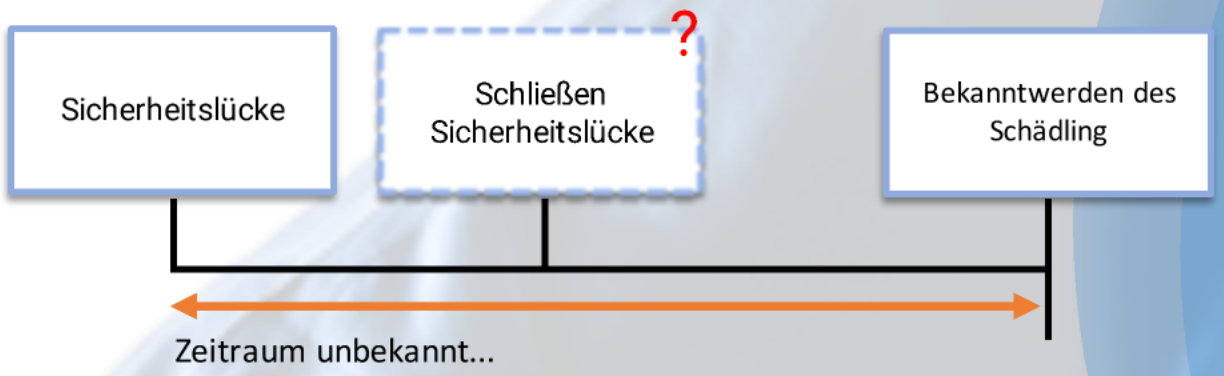
Systeme werden abgesichert

Typischer Verlauf eines Virenbefalles



- Virenschutz-Hersteller reagieren, Entwicklungszeitraum ungewiss
- Einige Sicherheitslücken werden niemals geschlossen

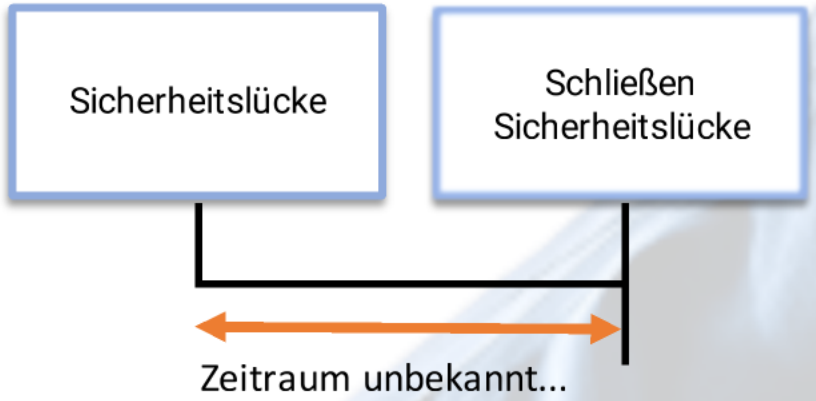
Typischer Verlauf eines Virenbefalls



- Nicht alle Sicherheitslücken werden frühzeitig erkannt!
- Nicht geschlossene Sicherheitslücken können angegriffen werden
- Ob und Wann ist ungewiss!

Systeme werden abgesichert

Typischer Verlauf eines Virenbefalls



- "Alle" IT-Systeme haben Sicherheitslücken
- Aufspüren von Sicherheitslücken ist Geschäftsmodell
- Schließen von Sicherheitslücken über Hersteller-Updates (Patches)
- Automatisierte Prozesse helfen!
- Nicht alle Sicherheitslücken werden frühzeitig erkannt!

Schädling wird bekannt

Warum
Sensibilisierung?

Ist unsere IT nicht
sicher genug?

Bedrohungslage

Bedrohungsarten

Grenzen technischer Hilfsmittel

(M)IT Sicherheit, geht mich das was an(!)?

IT-Sicherheit & die menschliche Firewall

Einstieg

Angriffspunkt Nr. 1:
Der Mensch

Praxistipps

Fragen?

für #zusammenwedemark Standortmarketing e.V.

Fachartikel

Der Faktor Mensch in der Cybersicherheit

Cybersicherheit ist nicht mehr länger nur ein Spezialthema, m
müssen. Alle Organisationen sind heute dazu gezwungen, sic
Cyberkriminelle haben nur ein Ziel: schnell Geld zu beschaffe

Universität Paderborn → Fakultäten → Fakultät für Elektrotechnik, Informatik und Mathematik → Informatik

21.12.2021 |

Cybersicherheit: Welche Rolle spielt der Faktor Mensch in einer digitalisierten Welt?

Paderborner Informatikerin erforscht menschenzentrierte Lösungen für verbesserte Sicherheitstechnologien

tuft das Bundesamt für Sicherheit in der Informationstechnik
n Deutschland in seinem jüngsten Jahresbericht ein. Durch
en, vermehrte cyber-kriminelle Erpressungsmethoden und
are Bereiche wie die medizinische Versorgung wächst die
gene Woche hat das BSI wegen einer Sicherheitslücke im
Programmiersprache Java die Warnstufe Rot ausgesprochen.
erheitsstrategien. Doch neueste Technik allein reicht nicht
ias-Cabarcos, die seit Oktober den Lehrstuhl für IT-Sicherheit
inne hat. Die Wissenschaftlerin rückt den Menschen auch in
us. Am Institut für Informatik erforscht sie, wie sich der
erheit durch menschenzentrierte Lösungen verbessern lässt.
lenschen sollen die Möglichkeit haben, ein sicheres digitales
iefgreifende technische Kenntnisse zu verfügen.

ms oder Teil der Lösung?

ich mehr und mehr auf digitale Infrastrukturen und Dienste.

Markt & Trends › Studien › Cybercrime: Die E-Mail ist Einfallstor Nummer eins

State of the Phish Report

Cybercrime: Die E-Mail ist Einfallstor Nummer eins

25.02.2022 | Von Ira Zahorsky

E-Mails sind nach wie vor die bevorzugte Angriffsmethode von Cyberkriminellen. Der Mitarbeiter bleibt damit der größte Risikofaktor. Gerade in puncto hybrides Arbeiten ist es wichtig, dass Unternehmen eine Sicherheitskultur aufbauen. Doch da klafft eine große Lücke.

Phishing" lässt sich bei zwei Dri
verbreitete Angriffsform. Ebens
(BEC, oder auch "Chefmasche"
erscheinen neue Bedrohungsfo
Verstecken bösartiger Payloads

Da eine Vielzahl gängiger Bedr
heutzutage nicht mehr in ein Ur
Anmeldedaten verschafft haber
lohnt ein genauerer Blick auf die
Schwachstelle abzielen, und wa
Finanzen effektiv zu schützen.

17.02.2020 • DIGITALISIERUNG IT-SICHERHEIT CYBERKRIMINALITÄT

Faktor Mensch ist weiterhin größtes Einfallstor für Cyberangriffe

Cyber-Sicherheitsrat Deutschland e.V. startet Schulungs- und Awareness-Plattform für Unternehmen

en

Der Cyber-Sicherheitsrat Deutschland e.V. und sein Mitglied, die Perseus Technologies GmbH bieten zukünftig ein gemeinsames Awareness- und Schulungsangebot für Cybersicherheit an. Zahlen des Gesamtverbands der Deutschen Versicherungswirtschaft e. V (2019) zufolge sind bei über 70 Prozent der Cyberangriffe E-Mails der Angriffsvektor und zielen gezielt auf den Menschen hinter dem Rechner.

Vor diesem Hintergrund setzt das Angebot den Fokus auf die Schulung von Mitarbeitenden und die Stärkung menschlicher Cybersicherheit. Interessierte Unternehmen können sich auf der Homepage des Cyber-Sicherheitsrat Deutschland e.V. für die Awareness-Schulung registrieren.

"Eine auf IT-Technik ausgelegte Sicherheitsstrategie reicht im Kampf gegen Cybersicherkriminalität nicht aus. Dazu gehört die Etablierung einer hierachieübergreifenden Sicherheitskultur," sagt Hans-Wilhelm Dünn, Präsident des Cyber-Sicherheitsrat Deutschland e.V. "Der Fokus der Ursachenforschung von

Ziele

- sensibler Umgang mit Unternehmensdaten
- Nutzen gängiger Sicherheitsfaktoren erkennen
- Gefahrenquellen erkennen

(M)IT Sicherheit, geht mich das was an(!)?

IT-Sicherheit & die menschliche Firewall

Einstieg

Angriffspunkt Nr. 1:
Der Mensch

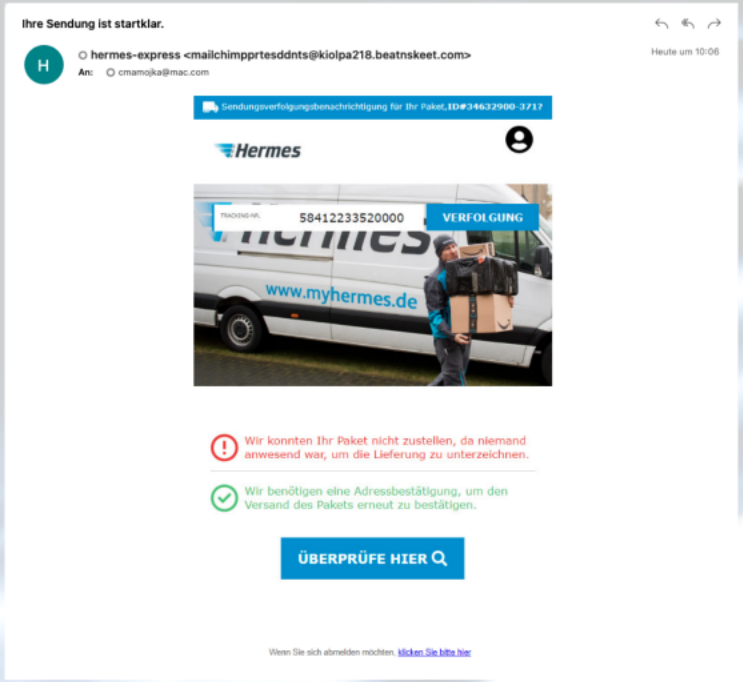
Praxistipps

Fragen?

für #zusammenwedemark Standortmarketing e.V.

Praxistipps

- schadhafte Email erkennen
- Social Engeneering
- Passwörter
- Zwei-Faktor-Anmeldung



An welchen typischen Merkmalen erkenne ich eine Phishing-Email?

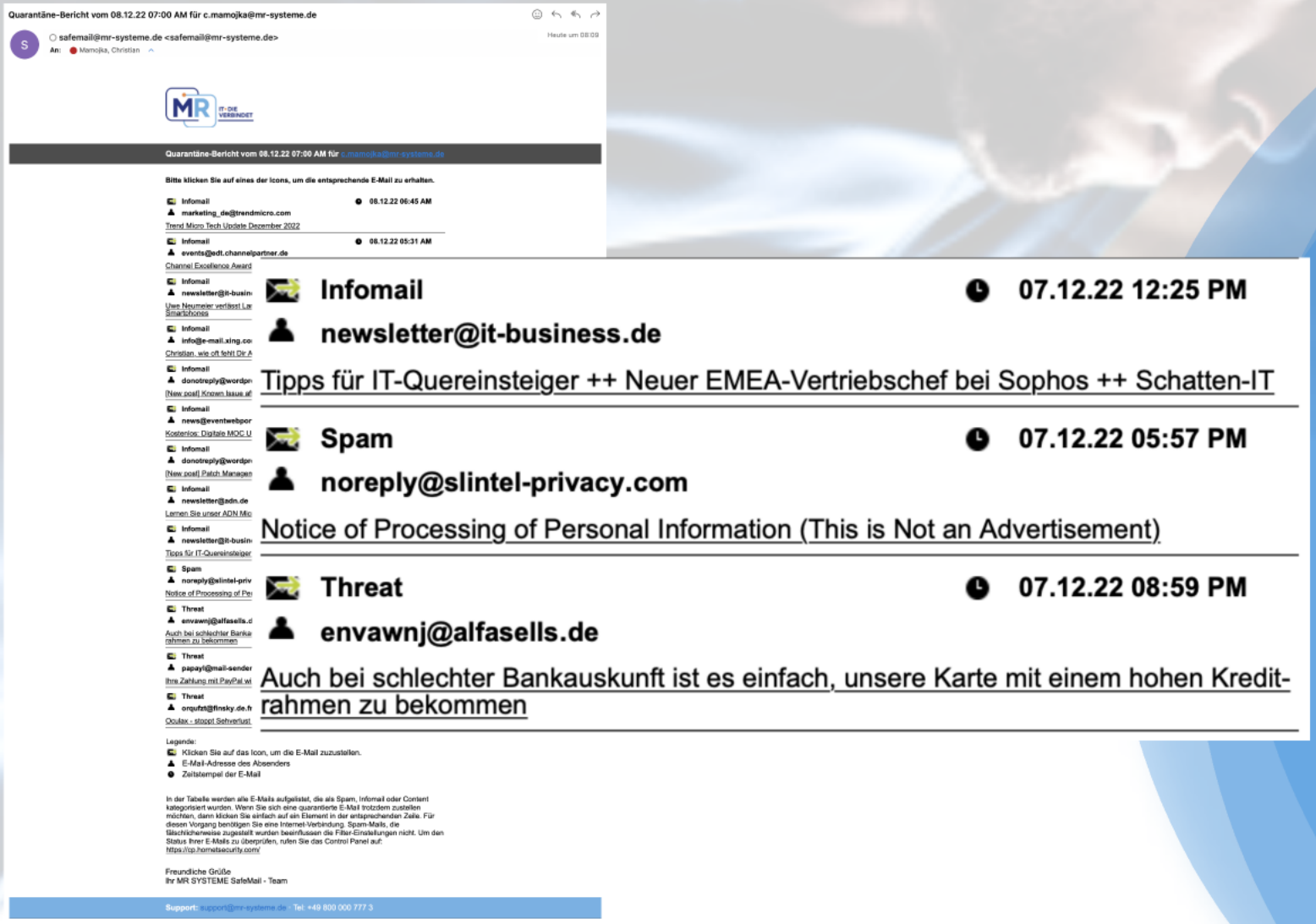
- Grammatikfehler
- fremde Sprache
- Name fehlt in Ansprache
- Dringender Handlungsbedarf
- Aufruf: Daten eingeben
- Link klicken

MR IT • DIE VERBINDET

Schadhafte Email erkennen

LIVE:
Phishing-Radar

Spamschutz



Quarantäne-Bericht vom 08.12.22 07:00 AM für c.mamojka@mr-systeme.de

safemail@mr-systeme.de <safemail@mr-systeme.de>
An: Mamojka, Christian

Heute um 08:09

Quarantäne-Bericht vom 08.12.22 07:00 AM für c.mamojka@mr-systeme.de

Bitte klicken Sie auf eines der Icons, um die entsprechende E-Mail zu erhalten.

Infomail — 08.12.22 06:45 AM
marketing_de@trendmicro.com
Trend Micro Tech Update Dezember 2022

Infomail — 08.12.22 05:31 AM
events@edt.channelpartner.de
Channel Excellence Award

Infomail
newsletter@it-busin
Uwe Neumeier verlässt La
Smartphones

Infomail
info@e-mail.xing.co
Christian, wie oft fehlt Dir A

Infomail
donotreply@wordpr
[New post] Known Issue af

Infomail
news@eventwebpor
Kostenlos: Digitale MOC U

Infomail
donotreply@wordpr
[New post] Patch Managen

Infomail
newsletter@adn.de
Lernen Sie unser ADN Mic

Infomail
newsletter@it-busin
Tipps für IT-Quereinsteiger

Spam
noreply@slintel-priv
Notice of Processing of Per

Threat
envawnj@alfasells.c
Auch bei schlechter Banka
rahmen zu bekommen

Threat
papayl@mail-sender
Ihre Zahlung mit PayPal wi

Threat
orqufzt@finsky.de.fr
Oculax - stoppt Sehverlust

Legende:
Klicken Sie auf das Icon, um die E-Mail zuzustellen.
E-Mail-Adresse des Absenders
Zeitstempel der E-Mail

In der Tabelle werden alle E-Mails aufgelistet, die als Spam, Infomail oder Content kategorisiert wurden. Wenn Sie sich eine quarantänierte E-Mail trotzdem zustellen möchten, dann klicken Sie einfach auf ein Element in der entsprechenden Zeile. Für diesen Vorgang benötigen Sie eine Internet-Verbindung. Spam-Mails, die fälschlicherweise zugestellt wurden beeinflussen die Filter-Einstellungen nicht. Um den Status Ihrer E-Mails zu überprüfen, rufen Sie das Control Panel auf:
https://cp.hornetsecurity.com/

Freundliche Grüße
Ihr MR SYSTEME SafeMail - Team

Support: support@mr-systeme.de - Tel: +49 800 000 777 3

Infomail — **07.12.22 12:25 PM**
newsletter@it-business.de
Tipps für IT-Quereinsteiger ++ Neuer EMEA-Vertriebschef bei Sophos ++ Schatten-IT

Spam — **07.12.22 05:57 PM**
noreply@slintel-privacy.com
Notice of Processing of Personal Information (This is Not an Advertisement)

Threat — **07.12.22 08:59 PM**
envawnj@alfasells.de
Auch bei schlechter Bankauskunft ist es einfach, unsere Karte mit einem hohen Kredit-rahmen zu bekommen

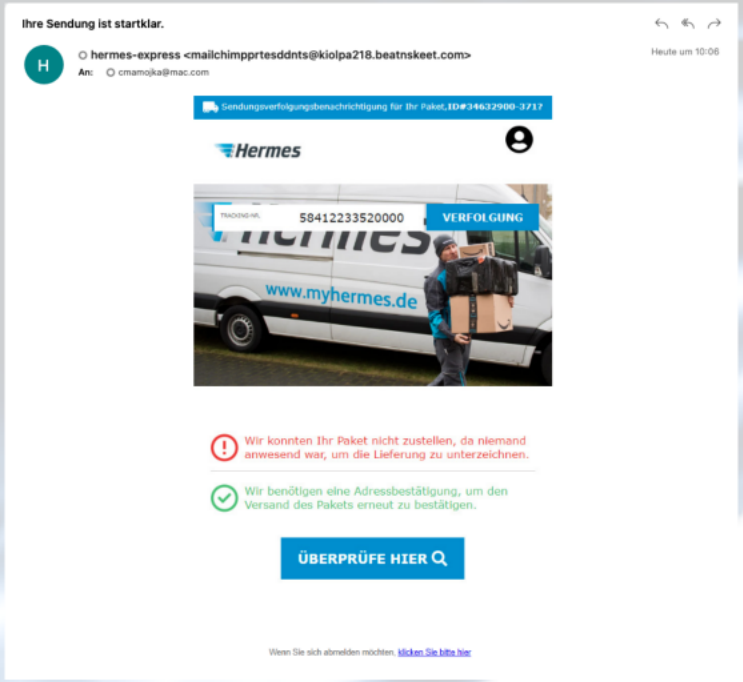
MR SafeExchange

Spam- und Virenschutz BEVOR das Unternehmensnetzwerk erreicht wird.

Live

Im SafeMail-Portal:

- Übersicht eingegangener Emails
- Freigabe als Spam markierter Emails
- Blacklist/Whitelist



An welchen typischen Merkmalen erkenne ich eine Phishing-Email?

- Grammatikfehler
- fremde Sprache
- Name fehlt in Ansprache
- Dringender Handlungsbedarf
- Aufruf: Daten eingeben
- Link klicken

MR IT • DIE VERBINDET

Schadhafte Email erkennen

LIVE:
Phishing-Radar

Spamschutz

Praxistipps

- schadhafte Email erkennen
- Social Engeneering
- Passwörter
- Zwei-Faktor-Anmeldung

Wie würden Sie reagieren?

„Hey, hier ist Christian aus der IT-Abteilung. Mir sind bei deinem Account in unserem System ein paar Unregelmäßigkeiten aufgefallen, kannst du mir einmal deine Zugangsdaten geben, damit ich das einmal überprüfen kann?"

Gruß Christian

Social Engeneering

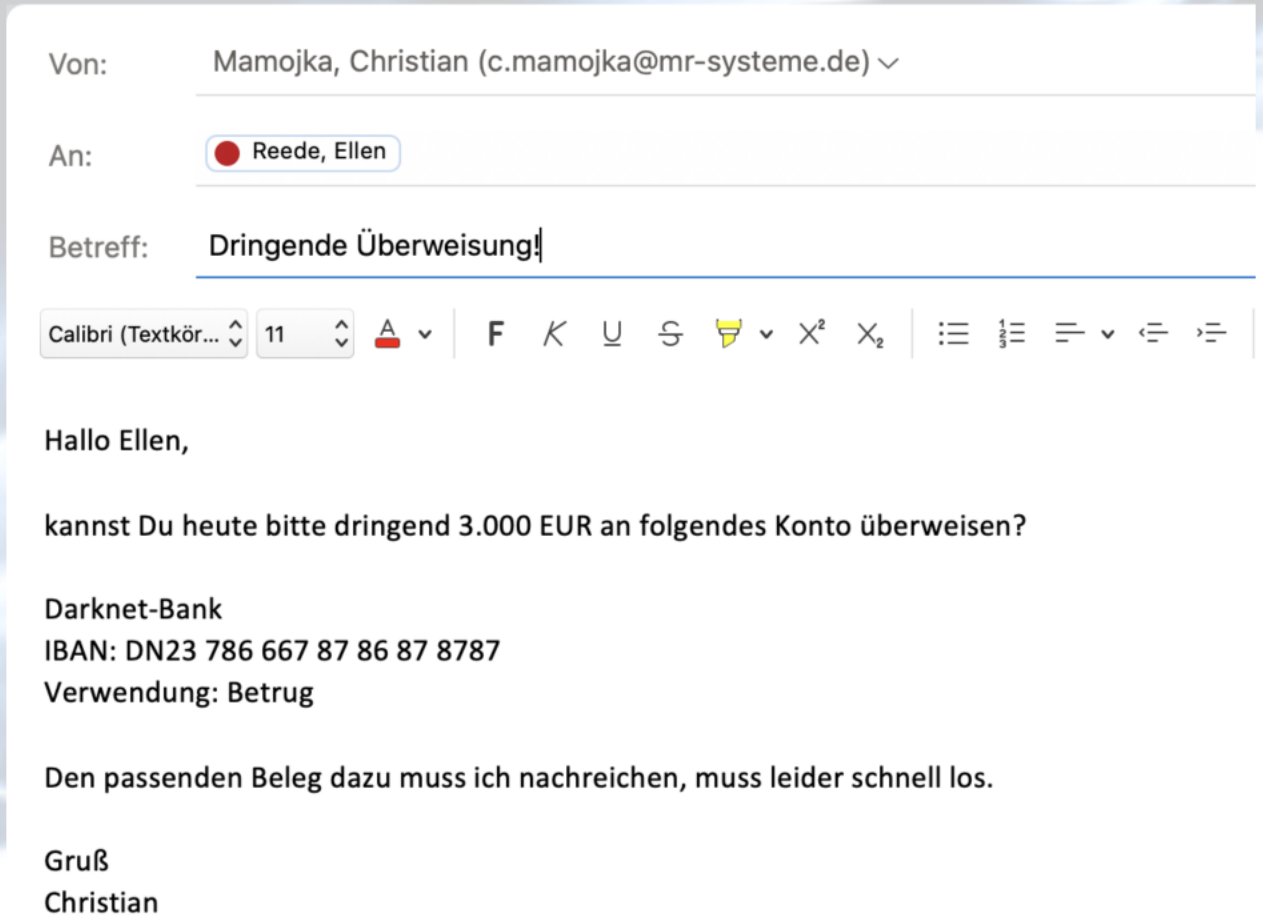
- zwischenmenschliche Beeinflussung einer Person
- eine Betrugsmasche, die schon seit vielen Jahrzenten genutzt wird
- eine der bekanntesten Maschen ist der Enkel-Trick

Social Engeneering in Unternehmen

Anrufe von extern Dienstleistern

Anrufe von extern

Gefälschte Email-Absenderadresse



Social Engeneering im Unternehmen

- Herangehensweise ist gängige Praxis im Unternehmen?
- Bestätigung via Telefon einholen

Wie würden Sie reagieren?

„Hey, hier ist Christian aus der IT-Abteilung. Mir sind bei deinem Account in unserem System ein paar Unregelmäßigkeiten aufgefallen, kannst du mir einmal deine Zugangsdaten geben, damit ich das einmal überprüfen kann?"

Gruß Christian

Social Engeneering

- zwischenmenschliche Beeinflussung einer Person
- eine Betrugsmasche, die schon seit vielen Jahrzenten genutzt wird
- eine der bekanntesten Maschen ist der Enkel-Trick

Social Engeneering in Unternehmen

Anrufe von extern Dienstleistern

Anrufe von extern

Ist der Anrufer vertrauenswürdig?

Social Engeneering
im Unternehmen

Anruf vom
- externen Dienstleister (MR Systeme)
- Software-Hersteller (Microsoft, Datev)
- Maschinenhersteller

Erbittet Zugriff auf Systeme via Fernwartung, **und jetzt?**

1. Rückrufnummer erfragen
   Auflegen
   Zurückrufen
2. Rückrufnummer erfragen
   Fachabteilung hinzuziehen
   Fachabteilung zurückrufen lassen
3. Identitätsnachweis anfordern

Wie würden Sie reagieren?

„Hey, hier ist Christian aus der IT-Abteilung. Mir sind bei deinem Account in unserem System ein paar Unregelmäßigkeiten aufgefallen, kannst du mir einmal deine Zugangsdaten geben, damit ich das einmal überprüfen kann?"

Gruß Christian

Social Engeneering

- zwischenmenschliche Beeinflussung einer Person
- eine Betrugsmasche, die schon seit vielen Jahrzenten genutzt wird
- eine der bekanntesten Maschen ist der Enkel-Trick

Social Engeneering in Unternehmen

Anrufe von extern Dienstleistern

Anrufe von extern

Welche Informationen geben Sie Preis?

Social Engeneering
im Unternehmen

Anruf von extern
"Guten Tag, hier spricht Herr Müller der 101-Consulting GmbH,
ist Herr Diedrichs zu sprechen?"

1. keine privaten Informationen

2. keine Auskunft über Grund und Länge von Abwesenheiten

Wie würden Sie reagieren?

„Hey, hier ist Christian aus der IT-Abteilung. Mir sind bei deinem Account in unserem System ein paar Unregelmäßigkeiten aufgefallen, kannst du mir einmal deine Zugangsdaten geben, damit ich das einmal überprüfen kann?"

Gruß Christian

Social Engeneering

- zwischenmenschliche Beeinflussung einer Person
- eine Betrugsmasche, die schon seit vielen Jahrzenten genutzt wird
- eine der bekanntesten Maschen ist der Enkel-Trick

Social Engeneering in Unternehmen

Anrufe von extern Dienstleistern

Anrufe von extern

Praxistipps

- schadhafte Email erkennen
- Social Engeneering
- Passwörter
- Zwei-Faktor-Anmeldung

Was muss ich im Umgang mit Passwörtern wissen?

- Komplexität
- Passwort nur einmal verwenden
- Nicht verraten
- Nicht aufschreiben
- Passwort durch zweiten Faktor schützen

Das perfekte Passwort:

X$GE(Ei<^(P=w5i#^AXQ3}]Sd8e}TDUMy

Wie lang muss mein Passwort sein?

- mindestens **10 Zeichen**

Bestehend aus:
+ kleinen Buchstaben
+ großen Buchstaben
+ Sonderzeichen
+ Ziffern

Warum?

Merkhilfen

Demo

Passwortgenerator mit Qualitätscheck

https://passwort-generator.org/

https://www.uni-muenster.de/ZIV.CERT/pw/index.php?lang=de&mode=pwcheck

Was muss ich im Umgang mit Passwörtern wissen?

- Komplexität
- Passwort nur einmal verwenden
- Nicht verraten
- Nicht aufschreiben
- Passwort durch zweiten Faktor schützen

Das perfekte Passwort:

X$GE(Ei<^(P=w5i#^AXQ3}]Sd8e}TDUMy

Wie lang muss mein Passwort sein?

- mindestens **10 Zeichen**

Bestehend aus:
+ kleinen Buchstaben
+ großen Buchstaben
+ Sonderzeichen
+ Ziffern

Warum?

Merkhilfen

Wie merke ich mir mein komplexes Passwort?

1. Passwortkarte
2. Merksatz
3. Aussprechbar

Kreativität

Welche Vorliebe haben Sie?

Für Whiskey-Liebhaber

Name + Alkoholgehalt + Preis = **Belvenie43%5990€**

Für Auto-Freunde

Marke + PS + CO2-Ausstoß = **VWTiguan130PS123g/km**

Für Schoki-Begeisterte

Marke + Kakaogehalt + Wochenkonsum **= Lindt70%1250gr**

Wie merke ich mir mein komplexes Passwort?

1. Passwortkarte
2. Merksatz
3. Aussprechbar

Kreativität

Was muss ich im Umgang mit Passwörtern wissen?

- Komplexität
- Passwort nur einmal verwenden
- Nicht verraten
- Nicht aufschreiben
- Passwort durch zweiten Faktor schützen

Das perfekte Passwort:

X$GE(Ei<^(P=w5i#^AXQ3}]Sd8e}TDUMy

Wie lang muss mein Passwort sein?

- mindestens **10 Zeichen**

Bestehend aus:
+ kleinen Buchstaben
+ großen Buchstaben
+ Sonderzeichen
+ Ziffern

Warum?

Merkhilfen

Praxistipps

- schadhafte Email erkennen
- Social Engeneering
- Passwörter
- Zwei-Faktor-Anmeldung

Was ist eine "Zwei-Faktor-Anmeldung"?

- Die Anmeldung mit einem "zweiten Passwort"

- Ein "zweites Passwort" kann sein
  - eine Zahlen-Kombination,
  - eine Rechenaufgabe,
  - ein Bilderrätsel oder

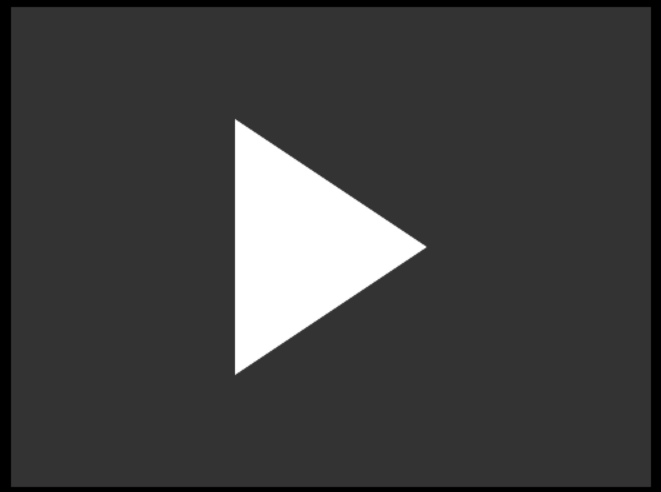
  biometrische Merkmale wie,
  - ein Fingerabdruck-Erkennung,
  - ein Iris-Erkennung,
  - ein Gesichts-Erkennung

  oder auch technische Hilfmittel wie
  - NFR-Chip (Token)
  - "App-gestützte"-Anmeldung

Erklärvideo des BSI

Beispiele

Fakten



Amazon

amazon.de

Zwei-Schritt-Verifizierung

Für zusätzliche Sicherheit gib bitte das Einmalkennwort (OTP) ein, das an eine Telefonnummer gesendet wurde, die auf 118 endet

OTP eingeben:

510093

☐ In diesem Browser nicht mehr nach Codes fragen

Anmelden

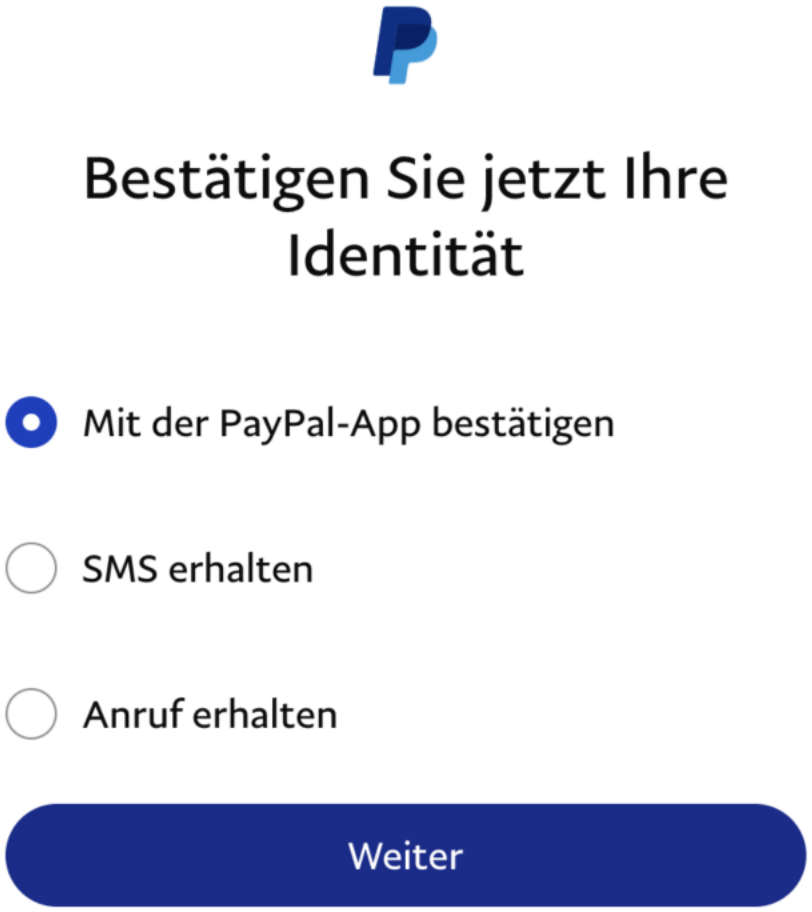
- Du hast das Einmalkennwort (OTP) nicht erhalten?

Datenschutzerklärung Hilfe Impressum Hinweise zu Cookies Hinweise zu interessenbasierter Werbung

OTP (One Time Password) gelangt via SMS oder EMail an den Benutzer.

Beispiel 2

PayPal

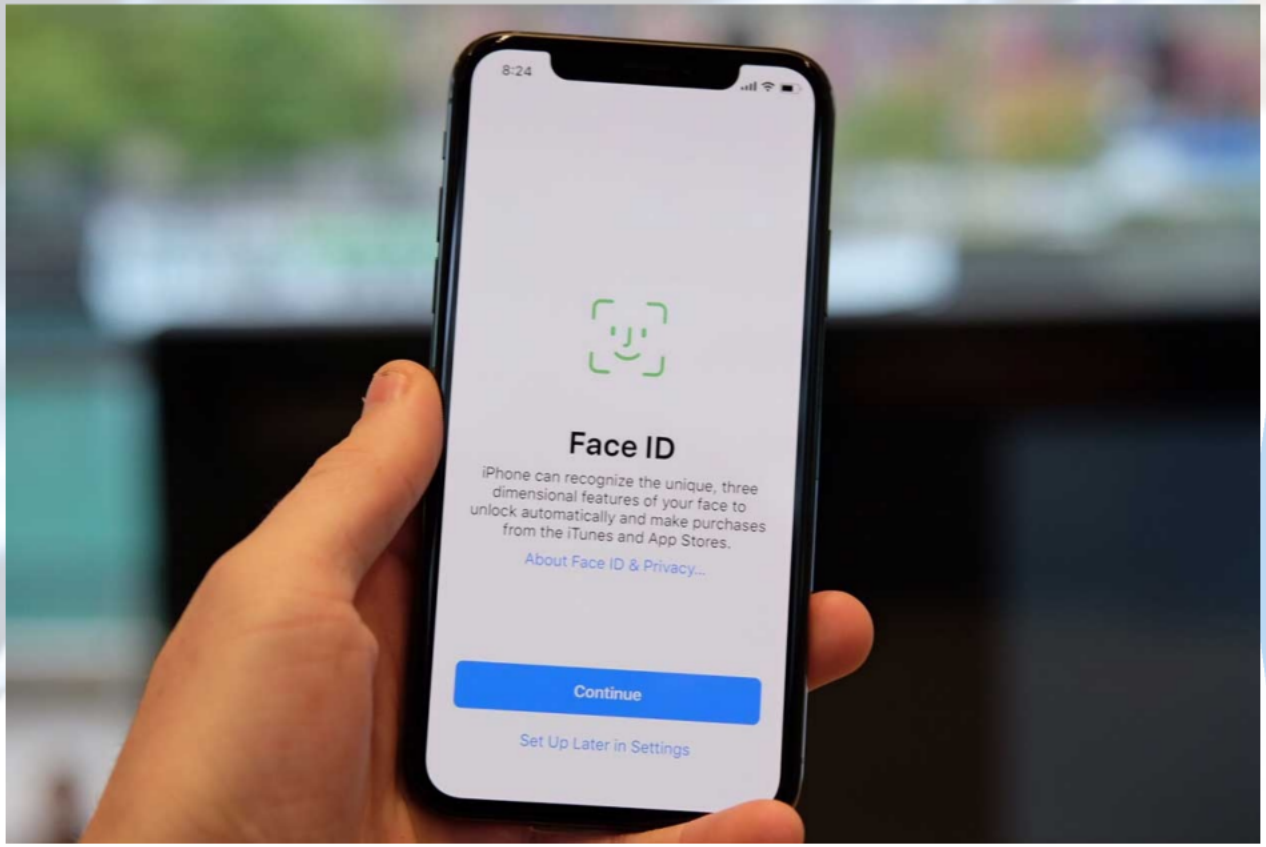


Auswahl mehrerer Möglichkeiten

- App-Authentifizierung
- SMS-Authentifizierung
- Anruf-Authentifizierung

Beispiel 3

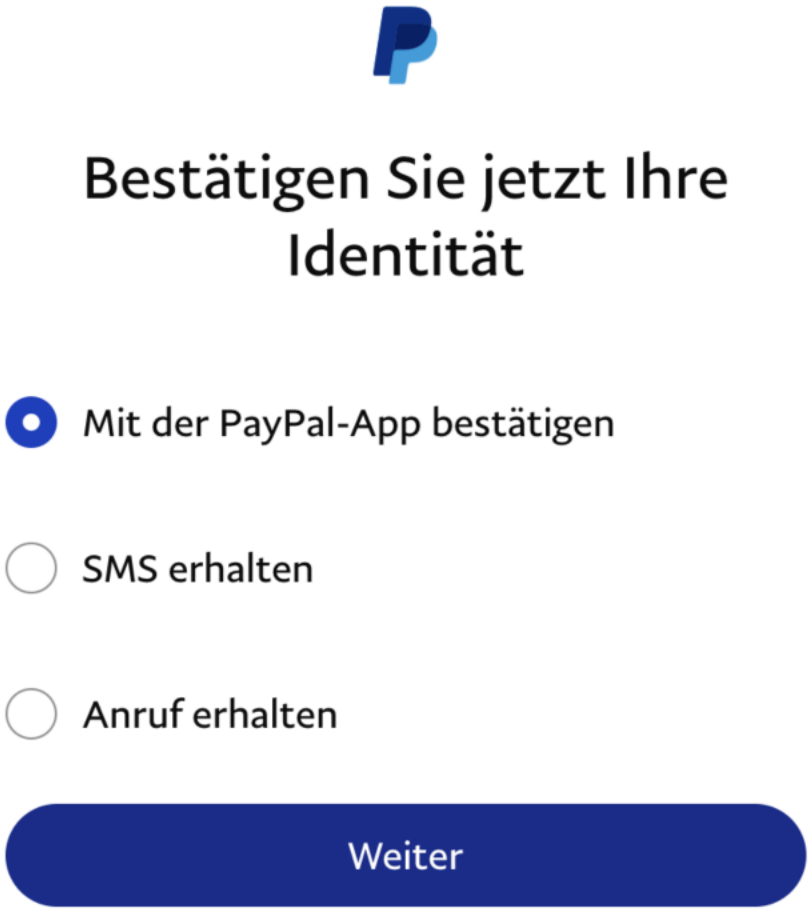
Apple



Gesichtserkennung statt PIN-Eingabe

- ersetzt in vielen Apps die Anmeldung via Passwort
- Passwort wird einmal eingegeben, danach nur noch Gesichterkennung

PayPal



Auswahl mehrerer Möglichkeiten

- App-Authentifizierung
- SMS-Authentifizierung
- Anruf-Authentifizierung

Beispiel 3

Amazon

amazon.de

Zwei-Schritt-Verifizierung

Für zusätzliche Sicherheit gib bitte das Einmalkennwort (OTP) ein, das an eine Telefonnummer gesendet wurde, die auf 118 endet

OTP eingeben:

510093

☐ In diesem Browser nicht mehr nach Codes fragen

Anmelden

- Du hast das Einmalkennwort (OTP) nicht erhalten?

Datenschutzerklärung Hilfe Impressum Hinweise zu Cookies Hinweise zu interessenbasierter Werbung

OTP (One Time Password) gelangt via SMS oder EMail an den Benutzer.

Beispiel 2

Was ist eine "Zwei-Faktor-Anmeldung"?

- Die Anmeldung mit einem "zweiten Passwort"

- Ein "zweites Passwort" kann sein
  - eine Zahlen-Kombination,
  - eine Rechenaufgabe,
  - ein Bilderrätsel oder

  biometrische Merkmale wie,
  - ein Fingerabdruck-Erkennung,
  - ein Iris-Erkennung,
  - ein Gesichts-Erkennung

  oder auch technische Hilfmittel wie
  - NFR-Chip (Token)
  - "App-gestützte"-Anmeldung

Erklärvideo des BSI

Beispiele

Fakten

Fakten zur "Zwei-Faktor-Anmeldung"?

- Im Zahlungsverkehr seit Jahren gängig PIN/TAN
- Pflicht im unternehmerischen Zahlungsverkehr, seit Mitte Januar 2021
- auch verpflichtend bei bspw. Apple, PayPal, Google oder Amazon
- deutlich höhere Sicherheit, aber kein 100%iger Schutz

Empfehlenswert:

Nutzen Sie es, wo immer es möglich ist!

Andere Bezeichnungen für die "Zwei-Faktor-Anmeldung"

- Zwei-Faktor-Authentifizierung
- Zwei-Faktor-Authentisierung
- 2FA
- OTP
- Multi-Faktor-Authentifizierung
- MFA

Was ist eine "Zwei-Faktor-Anmeldung"?

- Die Anmeldung mit einem "zweiten Passwort"

- Ein "zweites Passwort" kann sein
  - eine Zahlen-Kombination,
  - eine Rechenaufgabe,
  - ein Bilderrätsel oder

  biometrische Merkmale wie,
  - ein Fingerabdruck-Erkennung,
  - ein Iris-Erkennung,
  - ein Gesichts-Erkennung

  oder auch technische Hilfmittel wie
  - NFR-Chip (Token)
  - "App-gestützte"-Anmeldung

Erklärvideo des BSI

Beispiele

Fakten

Praxistipps

- schadhafte Email erkennen
- Social Engeneering
- Passwörter
- Zwei-Faktor-Anmeldung

(M)IT Sicherheit, geht mich das was an(!)?

IT-Sicherheit & die menschliche Firewall

Einstieg

Angriffspunkt Nr. 1:
Der Mensch

Praxistipps

Fragen?

für #zusammenwedemark Standortmarketing e.V.

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Sebastian Hoffmann
Vertriebsleiter und IT-Sicherheitsenthusiast
der MR Systeme GmbH am Standort Hannover

s.hoffmann@mr-systeme.de
0511 / 367 175 -30

https://www.mr-systeme.de

(M)IT Sicherheit, geht mich das was an(!)?

IT-Sicherheit & die menschliche Firewall

Einstieg

Angriffspunkt Nr. 1:
Der Mensch

Praxistipps

Fragen?

für #zusammenwedemark Standortmarketing e.V.