Sicherheits-Schulung für Endanwender

Sensibilisierung

Erkennung

Abwehr

von Cyber-Kriminalität

EVIATEC

Agenda

- Begrüßung, Vorstellung & Motivation
- Zahlen & Fakten
- Akteure & Ziele
- Chronologie eines Angriffs
- Phishing: Fangmethoden, Köder und Technik
- Beispiele
- Angriffe erkennen & abwehren
- Best Practices

Vorstellung

- EVIATEC Systems AG
  - Systemhaus, seit 20 Jahren am Markt
  - Spezialist für die Digitalisierung von Prozessen und ECM
  - Seit 5 Jahren verstärkt im Bereich Managed Security aktiv
- Bodo Schenk
  - Jahrgang 1976
  - Dipl. Informatik in Stuttgart
  - Netzwerktechnik und Anwendungsentwicklung

Motivation

- Kontinuierlicher Anstieg Cyberkriminalität in den letzten Jahren
- Zusätzliche Bedrohung durch Home Office / Mobile Workplaces
- Zunehmende Professionalisierung der Angreifer
- Vermehrt die Ausnutzung menschlichen Verhaltens („Social Engineering“)
- Öffentliche Einrichtungen und Hochschulen im Fokus

99% aller E-Mail basierten Angriffe setzen auf die Ausnutzung menschlichen Verhaltens

Proofpoint: „Human Factor Report 2019“

EVIATEC

Motivation

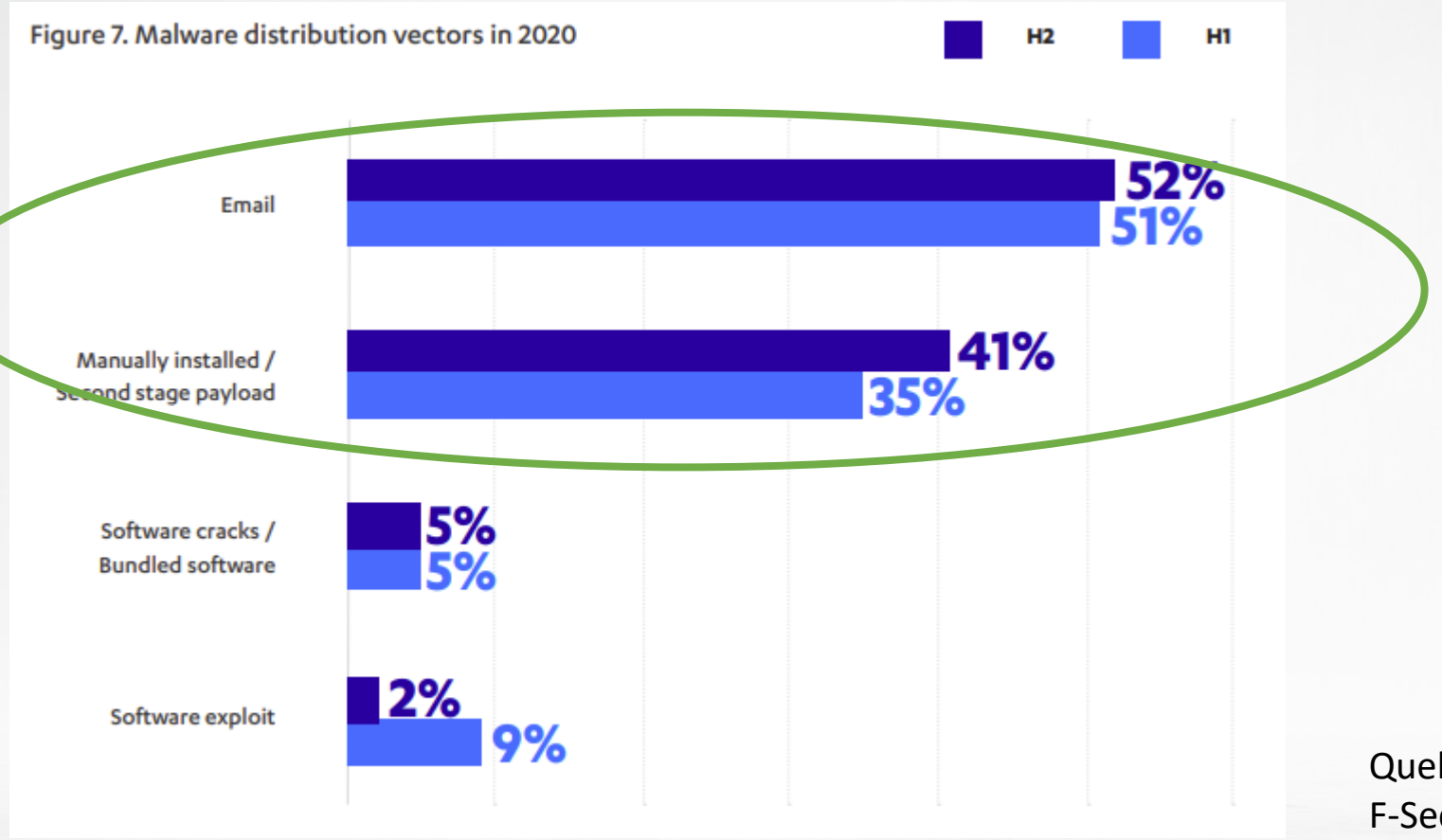
In den vergangenen zwei Jahren haben massive Angriffe auf Hochschulen mit teilweise langanhaltenden Folgen stattgefunden:

Berlin	Bochum	Dresden
Freiburg	Garching	Gießen
Heidelberg	Jülich	Karlsruhe
Köln	Leipzig	Nürnberg
Stuttgart	Weingarten	

Zahlen und Fakten

- BKA Lagebericht 2020 / Angezeigte Fälle
  - 2016: 82.649
  - 2017: 85.960
  - 2018: 87.106
  - 2019: 100.514
  - 2020: 108.474 (= 300 Fälle pro Tag !)

Wie kommen infizierte Dateien auf die PCs ?



Quelle:
F-Secure Attack Landscape
H1 2021

EVIATEC

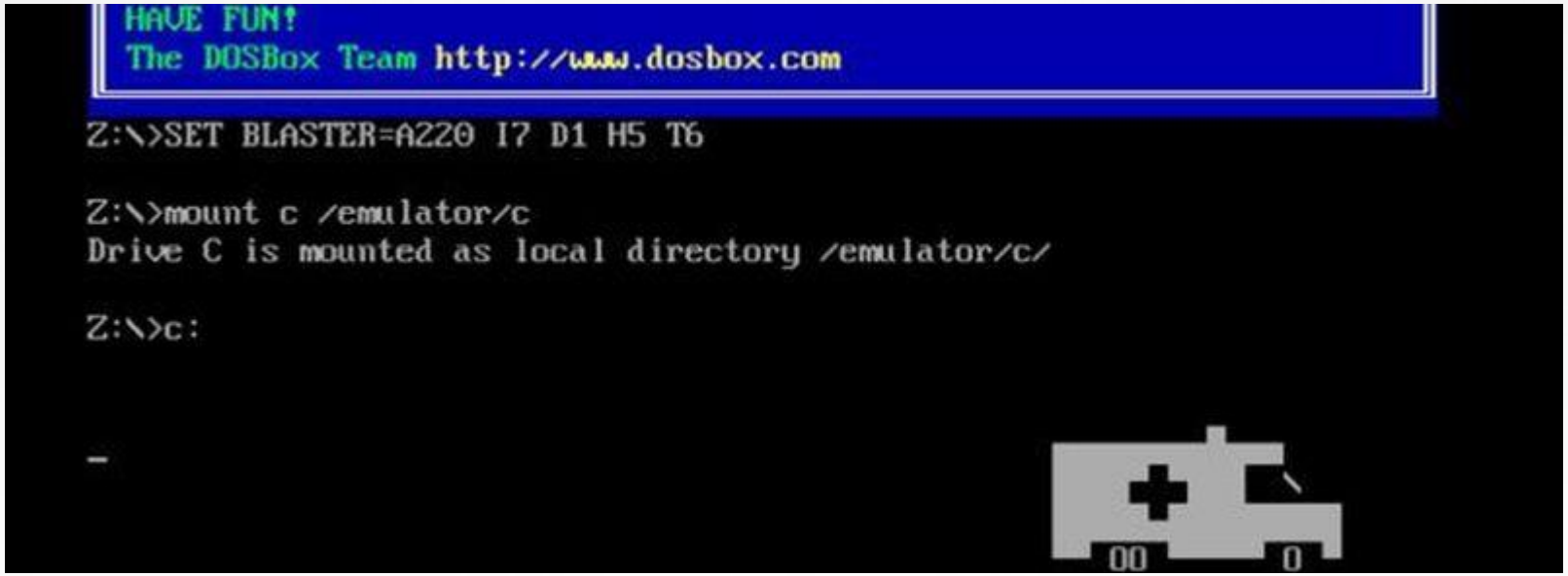
Lösegeldzahlungen

- Durchschnittlich gezahltes Lösegeld 2020: 300.000 $
- Durchschnittlich gefordertes Lösegeld 2020: 800.000 $
- Höchstes gezahltes Lösegeld 2020: 10.000.000 $
- Höchstes gefordertes Lösegeld 2020: 30.000.000 $
- Im Jahr 2019: 11,5 Milliarden US-Dollar Lösegeldzahlungen

Quellen:

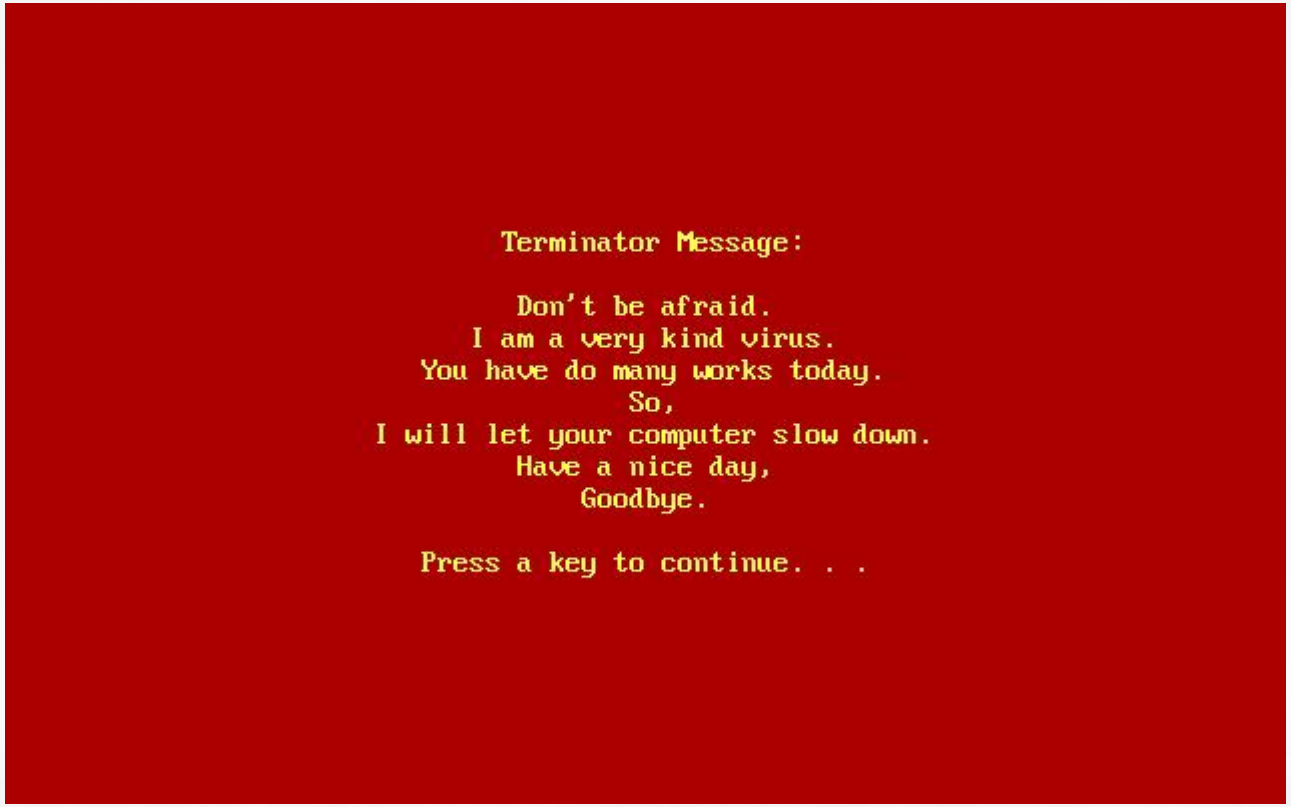
- Palo Alto Ransomware Threat Report 2021
- Acronis

Die guten alten Zeiten ...



EVIATEC

Skynet Virus (1994)



EVIATEC

Die Zeiten haben sich geändert

- Keine Einzelpersonen („Nerds“) mehr
- Internationale, staatlich unterstützte Hacker-Gruppen
- Extreme Professionalisierung
- Arbeitsteilung / Spezialisierung
- Lang vorbereitete, hochkomplexe Angriffe
  - z.B. „SunBurst“
  - 2 Jahre Vorbereitung
  - laut Microsoft waren über 1.000 Personen daran beteiligt
- Hilfestellung bei der Organisation der „Lösegeldübergabe“

Ziele von Cyber Kriminalität

- Erpressung von Lösegeld
  - Verschlüsselte Daten
  - Veröffentlichung von gestohlenen Daten
- Daten-/Technologiediebstahl
- Rechenleistung (Crypto-Mining)
  - CO2 für CryptoMining in China > kompletter Energiebedarf von Tschechien
- Identitätsdiebstahl
  - Übernahme von Accounts (Mail, Facebook, Amazon usw.)
  - Zahlreiche private Mailboxen von Studierenden sind gehackt
- Vortäuschung von Geschäftsvorgängen, z.B. bezahlen einer Rechnung ins Ausland

Ziele von Cyber Kriminalität

- Zunehmend Verlagerung auf
  - „Big Players“
  - öffentliche Einrichtungen
  - Kritische Infrastruktur
- Trotzdem ist man auch als kleines Unternehmen, als Verein oder als Privatperson nicht „sicher“ !

Bekannte Beispiele

- 2012/2016
  - Netzwerk LinkedIn
  - 167 Millionen Nutzerdaten 2012 geklaut
  - 2016 wurden sog. „gehashte“ Passwörter zum Verkauf angeboten
  - Mit einem hier geklauten Passwort konnte anschließend DropBox gehackt werden, da ein DropBox Mitarbeiter das gleiche Kennwort verwendet hat

Bekannte Beispiele

- 2017 WannaCry
  - Windows-Sicherheitslücke „EternalBlue“
  - Wurde ursprünglich von der NSA entdeckt und ausgenutzt
  - Kam dann in die Hände einer Hacker-Gruppe
  - Infizierung mehrerer 100.000 Computer in über 150 Ländern
  - Bekannte durch Ausfall der Anzeigetafeln der Deutschen Bahn
  - Lösegelderpressung
  - Windows-Sicherheitsupdate war schon zwei Monate vorher verfügbar
  - Auch 2020 noch über eine Million Windows-Geräte anfällig

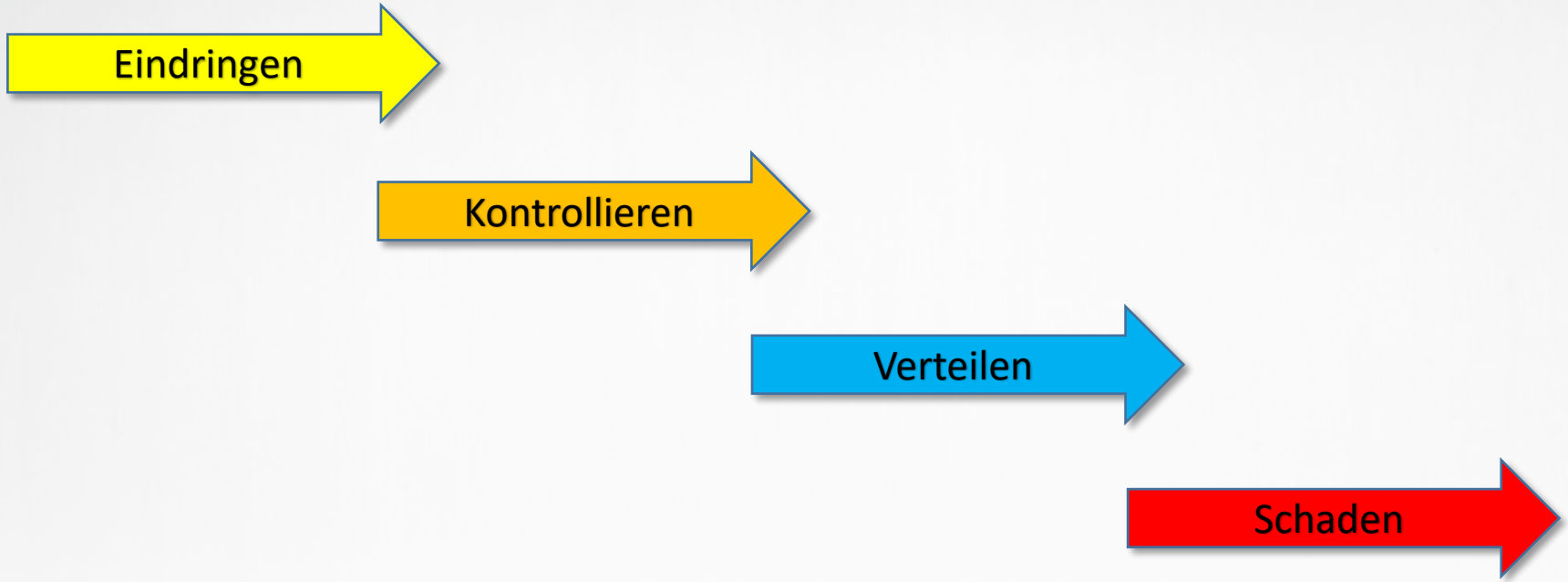
Bekannte Beispiele

- September 2020
  - Universitätsklinikum Düsseldorf
  - 100.000 Patientenakten gestohlen
  - Notaufnahme geschlossen, Patienten auf andere Krankenhäuser verteilt
  - Eine Patientin stirbt in einem umgeleiteten Krankenwagen
  - Angriff galt nicht der Klinik, sondern der Heinrich-Heine-Universität
  - Angreifer gaben den Verschlüsselungs-Code freiwillig zurück

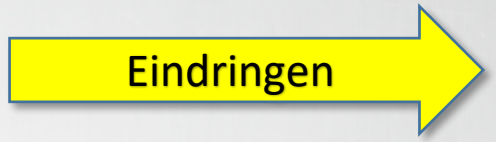
Bekannte Beispiele

- Mai 2021
  - Pipeline-Betreiber Colonia
  - Pro Tag 400 Millionen Liter Benzin für die Ostküste der USA
  - Versorgungsengpässe, Tankstellen geschlossen
  - Unternehmen zahlt 4,4 Millionen Dollar Lösegeld

Chronologie eines Angriffs



1) Eindringen



Der Angreifer benötigt einen ersten Einstiegspunkt in das Netzwerk des Opfers („Fuß in der Tür“).

- Sicherheitslücken in öffentlich zugänglichen Diensten (OWA, RDP usw.)
- Fernzugriff (VPN, Citrix, RDP) mit gestohlenen/erratenen Kennwörtern
- Unsicheres WLAN
- Physikalischer Zugang zu Netzwerkgeräten
- USB-Sticks/CDs
- Social Engineering (E-Mail, Telefon)
- Kompromittierter Mitarbeiter

EVIATEC

Fangmethoden

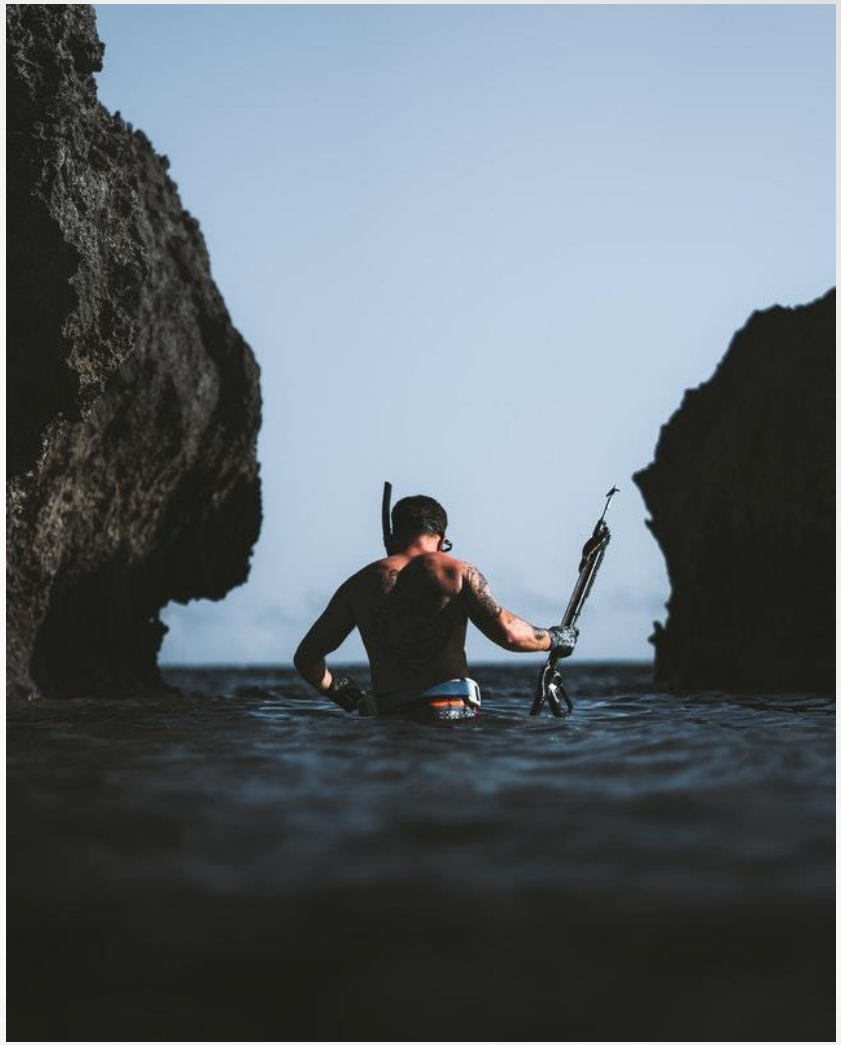
„Klassisches“ Phishing

- Große Massen an E-Mails
- Wenig Individualität
- Oftmals leicht zu erkennen
- Ansprache/Stil/Form/Rechtschreibung verdächtig

Fangmethoden

Spear Phising

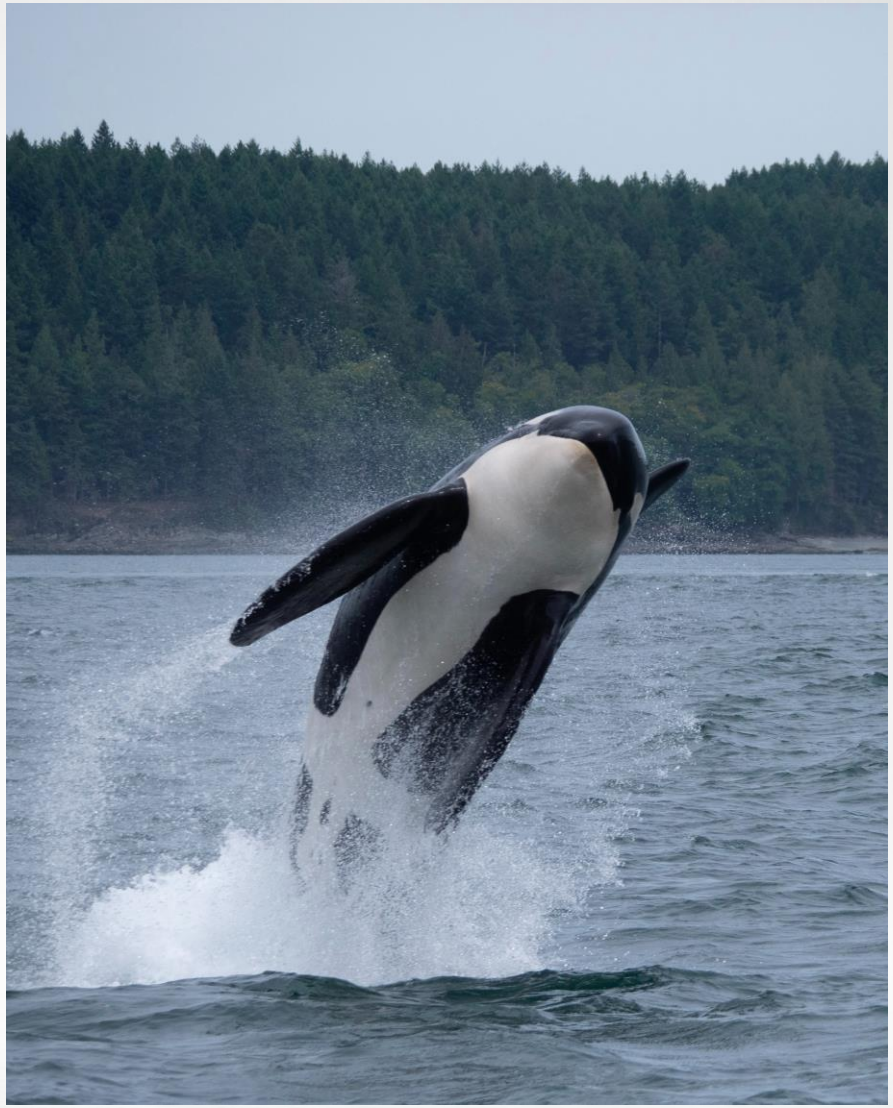
- Gezielter Angriff auf einen einzelnen Fisch
- Analyse alter E-Mails
  - Gehen Sie davon aus, dass Angreifer Zugriff auf die Mails von Studierenden haben
- Informationen über Opfer
  - Social Media
  - Unternehmens-Webseite
- Thematisieren von echten Vorgängen
- Imitation von Form und Stil



Fangmethoden

Whale Phising

- Angriff auf einen „großen“ Fisch
- Geschäftsführung
- Buchhaltung
- „CEO Fraud“



Fangmethoden

Voice Phishing

- Telefonanruf
- Vertrauensbildend durch persönliche Ansprache
- Druckausübung („können wir doch schnell machen es ist dringend“)
- Angreifer melden sich z.B. als „Microsoft Support“
- Aktuelle Infos auch zu finden unter
  https://www.ph-ludwigsburg.de/hochschule/einrichtungen/mit/it-sicherheit

Fangmethoden

SMS Phishing

- Auch in einer SMS können sich Links befinden, die auf modernen Smartphones geöffnet werden können
- Manche Telefone können auch über speziell codierte SMS-Nachrichten ferngesteuert werden
- Absender-Nummer kann gefälscht werden
- Für SMS gilt das gleiche wie für E-Mails, übrigens genauso:
  - WhatsApp-Nachrichten
  - Facebook Messenger
  - Zoom
  - usw.

Der Köder

- Mitteilung „unter Kollegen“ (Bsp.: WM-Tippspiel)
- "Offizielle" Mitteilung (Bsp.: Weihnachtsfeier)
- CEO Fraud (Angreifer gibt sich als Geschäftsführer aus)
- Bezugnahme auf aktuellen Vorgang (Bsp.: Bestellung)
- Nutzung von allgemein bekannten „Brands“ (DHL, PayPal, Sparkasse, Microsoft usw.) (Bsp.: Paketversand)
- Persönliche Notlagen (Bsp.: Geldbeutel geklaut)
- Aktuelle Themen (Bsp.: Corona, Flutopfer, Sicherheitslücken)
- Drohszenarien (Bsp.: bestätigen sie sofort ihr Kennwort sonst werden alle Konten gesperrt)

Phishing Techniken

Anhang an der E-Mail

- im Anhang befindet sich eine infizierte Datei
- evtl. versteckt in einer ZIP Datei
- enthält „Makros“ oder andere ausführbare Skripte
- Diese laden dann die eigentliche Schadsoftware von einem C&C-Server nach

Phishing Techniken

Link innerhalb der E-Mail

- Ziel des Links ist eine infizierte Webseite
- Webseite nutzt Sicherheitslücken in Internet-Browsern aus, um Schadsoftware zu installieren
- Webseite verleitet zur Installation eines infizierten Programms
- Webseite verleitet zur Eingabe von Kennwörtern, PINs usw.
- Achtung: Text des Links und „echter“ Link können voneinander abweichen (mit der Maus ohne zu Klicken über den Link fahren)

Phishing Techniken

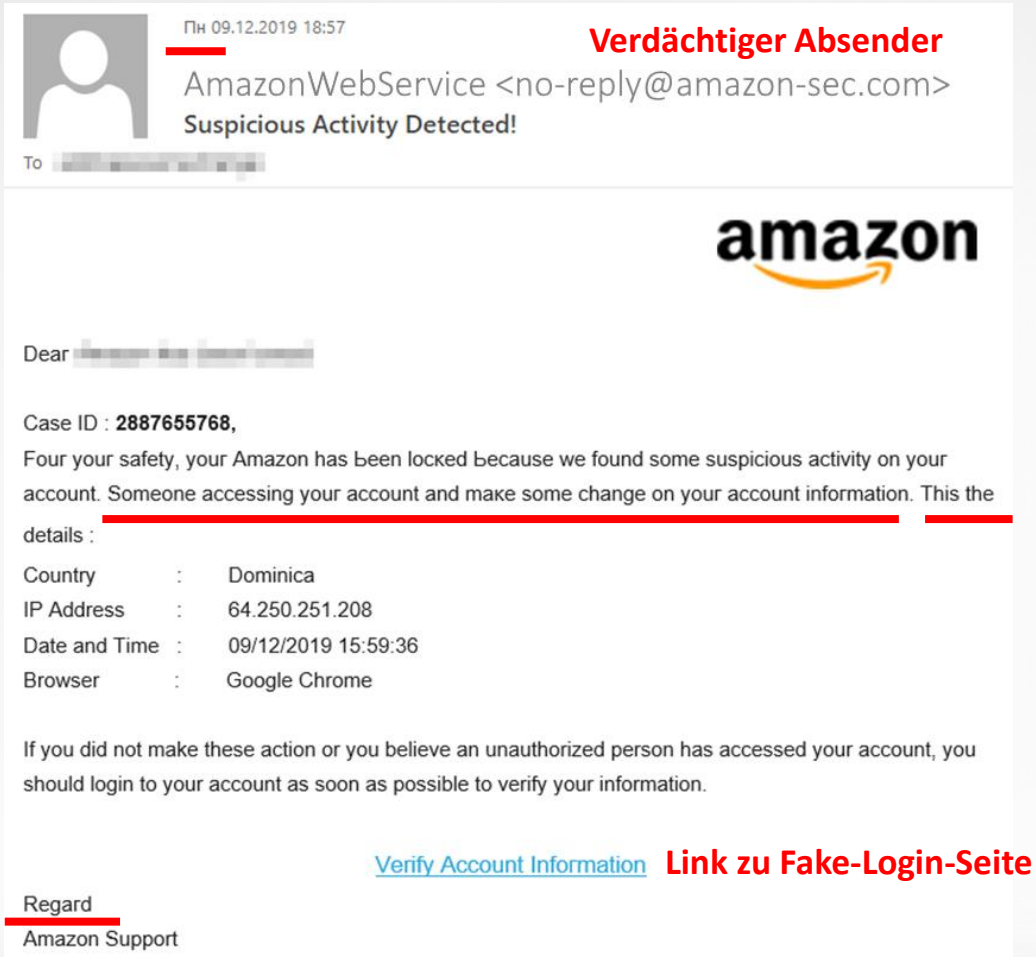
Fake-Login Seite

- Täuschend echt nachgebaut (für den Laien nicht erkennbar)
- Eingabe von Benutzername und Kennwort
- Das Benutzerkonto wird vom Angreifer übernommen
- Oftmals viele Wochen/Monate unentdeckt
- Übernahme weiterer Systeme (gleiche Kennwörter)
- Nutzung des Kontos für Angriffe auf Bekannte/Geschäftspartner
- „Identitätsdiebstahl“

Beispiele

- Die folgenden Beispiele sind alle in dieser (oder ähnlicher) Form bereits an der PH aufgetreten
- Es handelt sich also um eine echte, konkrete Bedrohungslage
- Einige Beispiele kommen auch direkt aus meinem beruflichen und privaten Alltag

Beispiele



Пн 09.12.2019 18:57

Verdächtiger Absender

AmazonWebService <no-reply@amazon-sec.com>

Suspicious Activity Detected!

To [redacted]

amazon

Dear [redacted]

Case ID : **2887655768,**

Four your safety, your Amazon has been locked because we found some suspicious activity on your account. Someone accessing your account and make some change on your account information. This the details :

Country	:	Dominica
IP Address	:	64.250.251.208
Date and Time	:	09/12/2019 15:59:36
Browser	:	Google Chrome

If you did not make these action or you believe an unauthorized person has accessed your account, you should login to your account as soon as possible to verify your information.

Verify Account Information **Link zu Fake-Login-Seite**

Regard

Amazon Support

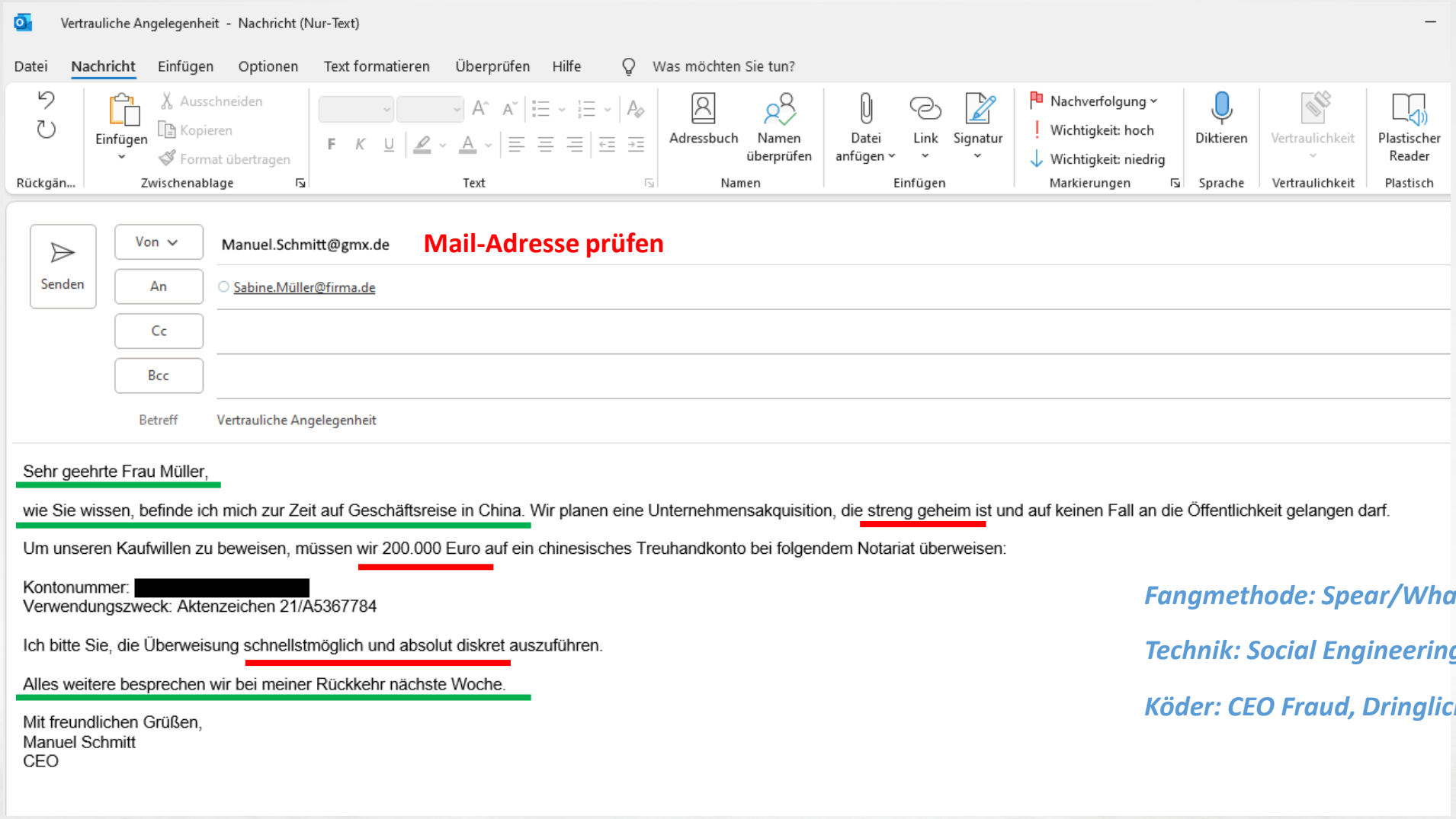
Fangmethode: klassisches Phishing

Technik: Link zu Fake-Seite

Köder: Bekannter Brand, Drohszenario

EVIATEC

Beispiele



Fangmethode: Spear/Whale Phishing

Technik: Social Engineering

Köder: CEO Fraud, Dringlichkeit

EVIATEC

Beispiele

Persönlich bekannt ?
Telefonnr. plausibel ?

„Guten Tag Frau Müller, hier spricht Manuel Schmitt aus der IT-Abteilung. Ich habe hier ein Ticket von Ihnen zur Bearbeitung, ist das Problem denn noch vorhanden ?“

Ticketnummer ?

„Können Sie mir das Problem noch einmal beschreiben ?“

„Ok, ich schalte mich ganz kurz auf Ihren PC, um mir das einmal selber anzuschauen. Haben Sie denn den Teamviewer schon installiert ?“

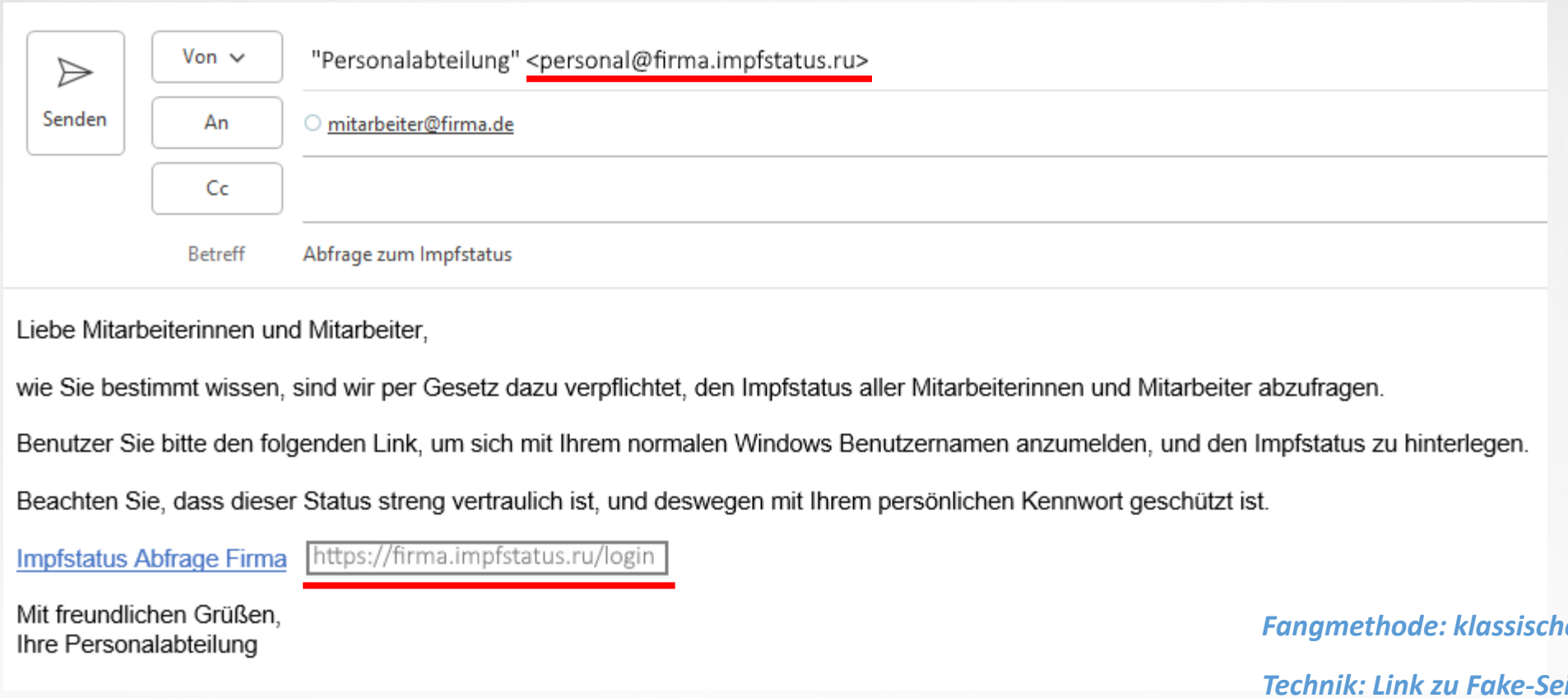
Wird der Bildschirm schwarz geschaltet ?
Wird etwas heruntergeladen/installiert/ausgeführt ?

Fangmethode: Voice Phishing

Technik: Social Engineering

Köder: Aktueller Vorgang

Beispiele



Senden

Von "Personalabteilung" <personal@firma.impfstatus.ru>

An mitarbeiter@firma.de

Cc

Betreff Abfrage zum Impfstatus

Liebe Mitarbeiterinnen und Mitarbeiter,

wie Sie bestimmt wissen, sind wir per Gesetz dazu verpflichtet, den Impfstatus aller Mitarbeiterinnen und Mitarbeiter abzufragen.

Benutzer Sie bitte den folgenden Link, um sich mit Ihrem normalen Windows Benutzernamen anzumelden, und den Impfstatus zu hinterlegen.

Beachten Sie, dass dieser Status streng vertraulich ist, und deswegen mit Ihrem persönlichen Kennwort geschützt ist.

Impfstatus Abfrage Firma https://firma.impfstatus.ru/login

Mit freundlichen Grüßen,
Ihre Personalabteilung

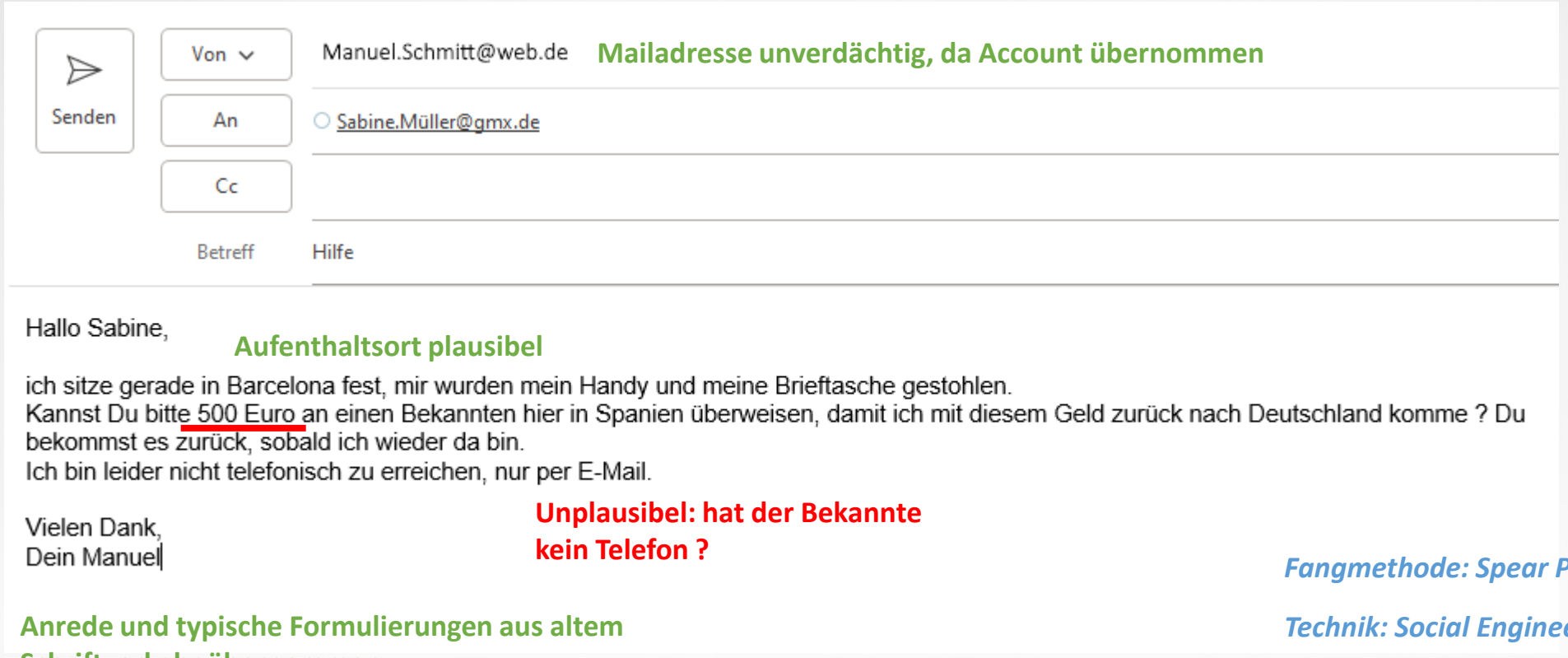
Fangmethode: klassisches/Spear Phishing

Technik: Link zu Fake-Seite

Köder: Aktuelles Thema (3G-Regel), Offizielle Mitteilung

EVIATEC

Beispiele



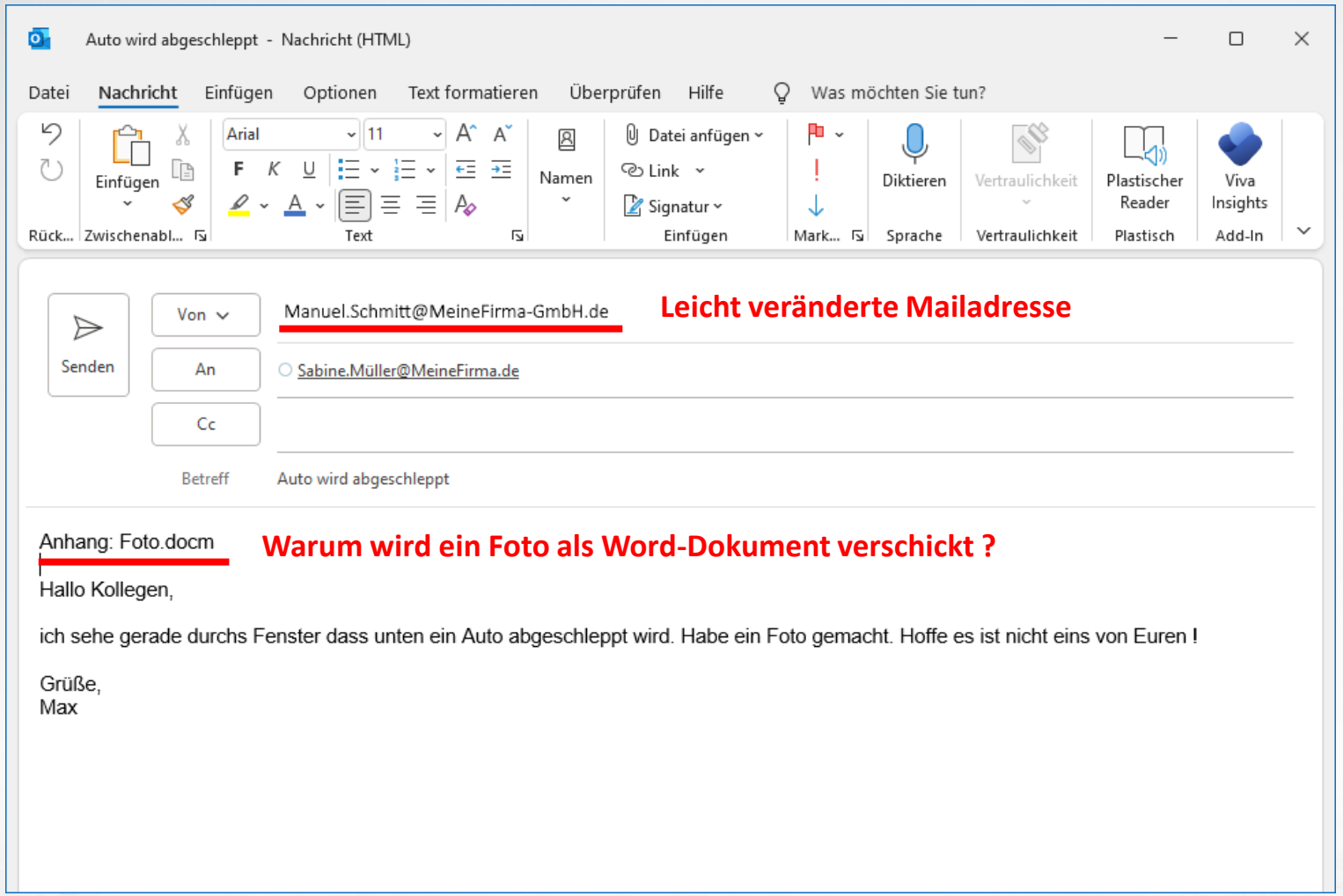
Fangmethode: Spear Phishing

Technik: Social Engineering

Köder: Persönliche Notlage

EVIATEC

Beispiele



Fangmethode: klassisches/Spear Phishing

Technik: Dateianhang

Köder: Mitteilung unter Kollegen

EVIATEC

Beispiele

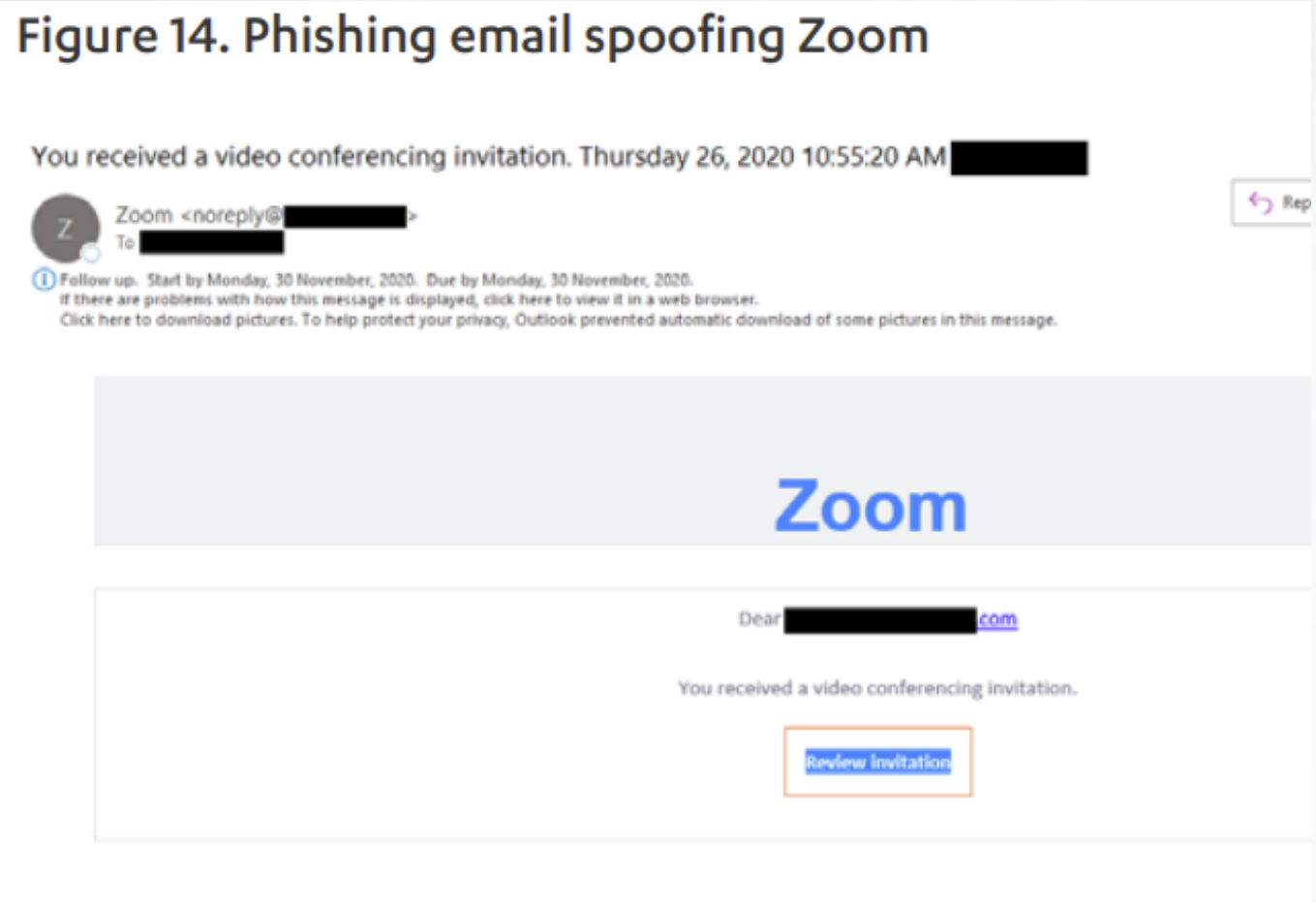
Fangmethode: klassisches Phishing

Technik: Link zu Fake-Seite

Köder: Bekannter Brand

EVIATEC

Beispiele



Fangmethode: klassisches Phishing

Technik: Link zu Fake-Seite

Köder: Bekannter Brand

EVIATEC

Angriffe erkennen & abwehren

- Prüfen Sie immer:
  - Rechtschreibung, Ausdruck, Stil und Form
  - Inhalt und Plausibilität
  - Mailadressen
  - Links
  - URL und Zertifikat von Login-Eingabemasken
- Achtung:
  - Der angezeigte Link kann sich vom Echten unterscheiden
  - Die angezeigte Mailadresse kann sich von der Echten unterscheiden

Angriffe erkennen & abwehren

- Nicht nur die E-Mail selbst, sondern auch Anhänge (PDF, Bilder usw.) können gefälscht/verfälscht worden sein
- Werden Sie misstrauisch, sobald
  - ... jemand versucht, Sie unter Druck zu setzen
  - ... es „dringend“ oder „geheim“ ist
  - ... es um Geld geht
  - ... es um Kennwörter, PINs, Kreditkarten usw. geht
- Versichern Sie sich immer persönlich bei einer Ihnen bekannten Person

Angriffe erkennen & abwehren

- Seriöse Partner fragen niemals nach Kennwörtern, PINs usw.
- Ausnahme: die offizielle Login-Seite des Anbieters
- Tipp: speichern Sie die offiziellen (sicheren) Login-Seiten als Favorit
- Lassen Sie keine unbekannten Personen an oder auf ihren PC
- Vorsicht mit USB-Sticks, CDs usw.
    - Schon das Einstecken/Einlegen kann zur Infektion führen („AutoRun“)

Prüfen eines Links / einer URL

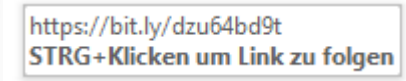
- Prüfen Sie immer, wo genau ein Link hingeht
- Fahren Sie mit der Maus über den Link, ohne zu klicken
- Die letzten beiden Teile des Links sind maßgeblich
- Nur HTTPS ist verschlüsselt
- Vorsicht: HTTPS ist nicht automatisch vertrauenswürdig !

Prüfen eines Links / einer URL

OK

facebook.ru statt facebook.com, kein HTTPS

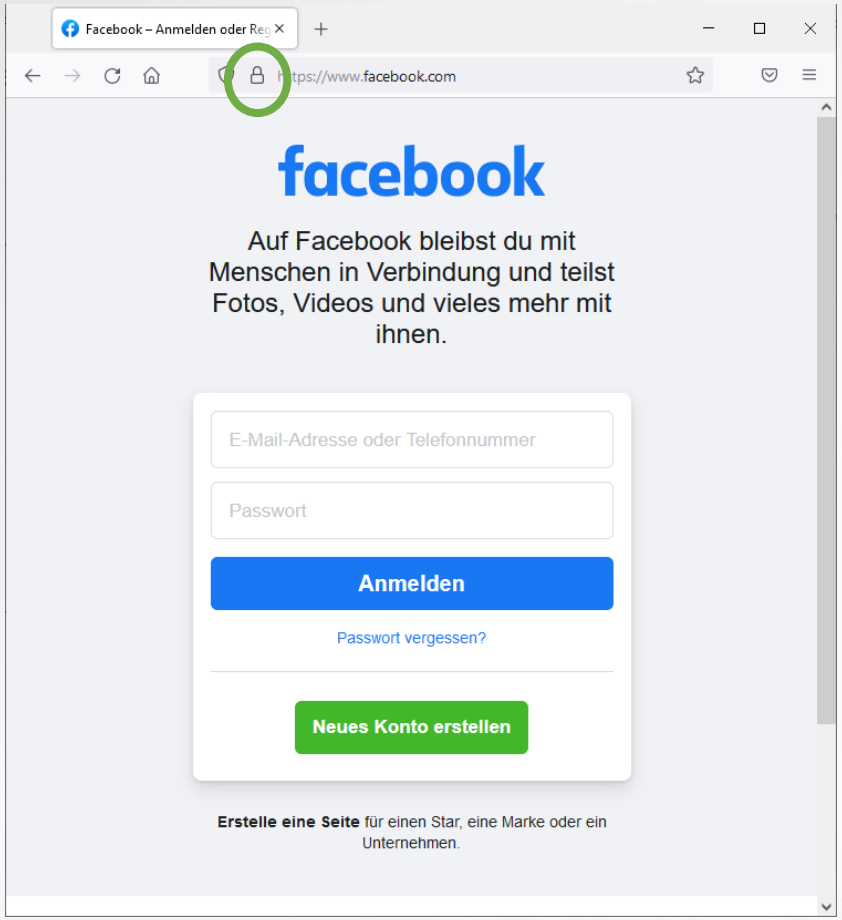
loginpage.com statt facebook.com



Link-Shortener (Ziel unbekannt)

EVIATEC

Prüfen eines Zertifikats

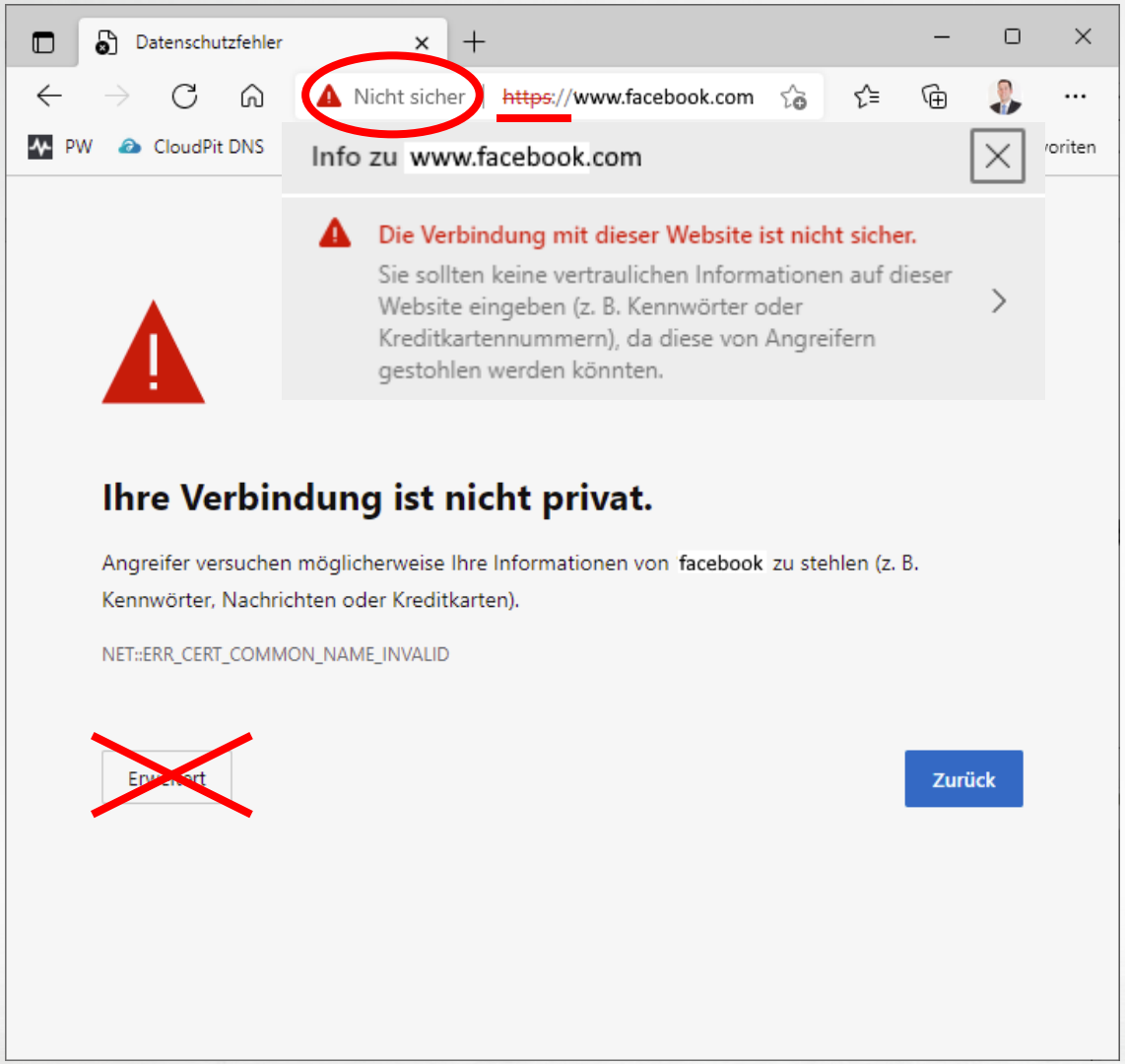


Firefox

Chrome

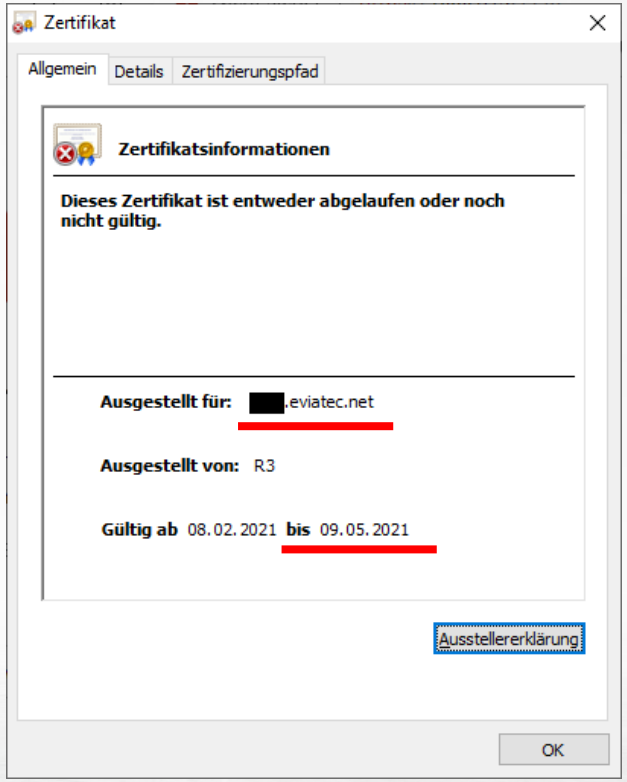
Die angezeigte Seite passt zur URL im Browser.

Prüfen eines Zertifikats



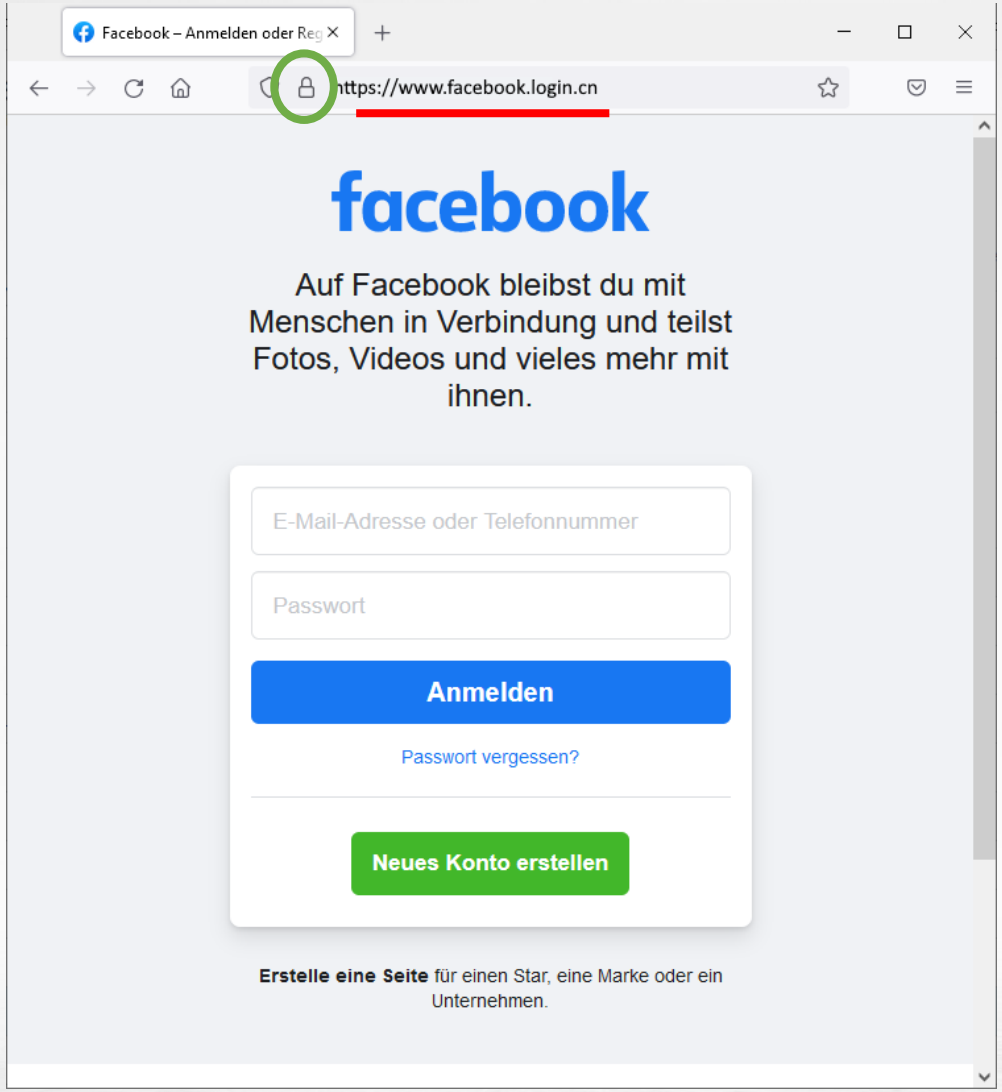
Edge

Die angezeigte Seite passt nicht zur URL im Browser.



EVIATEC

Prüfen eines Zertifikats



Der Angreifer hat sich ein zu seiner Fake-Seite passendes Zertifikat erstellt.

-> Die Fake-Seite passt zur Fake-URL !

EVIATEC

Prüfen eines Zertifikats

Nur wenn ...

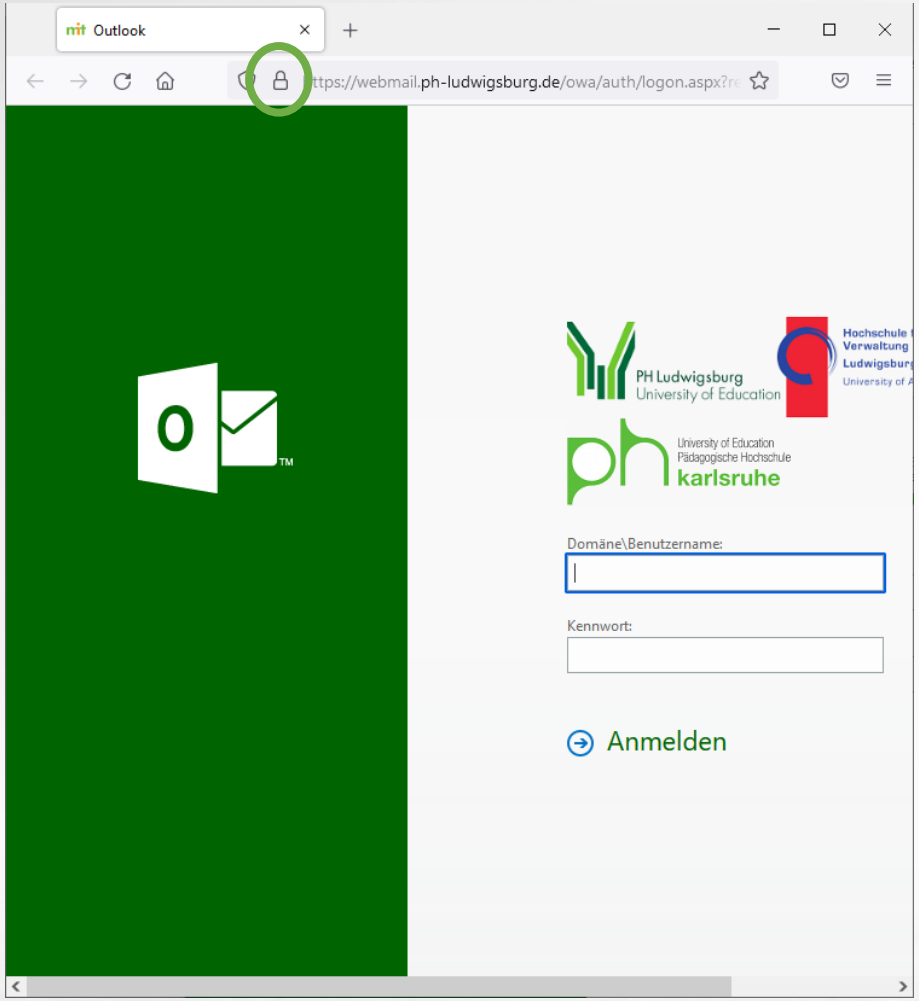
die im Browser angezeigte URL stimmt

und

das Zertifikat-Symbol ok ist

... ist die Seite (vermutlich) sicher.

Prüfen eines Zertifikats



Firefox

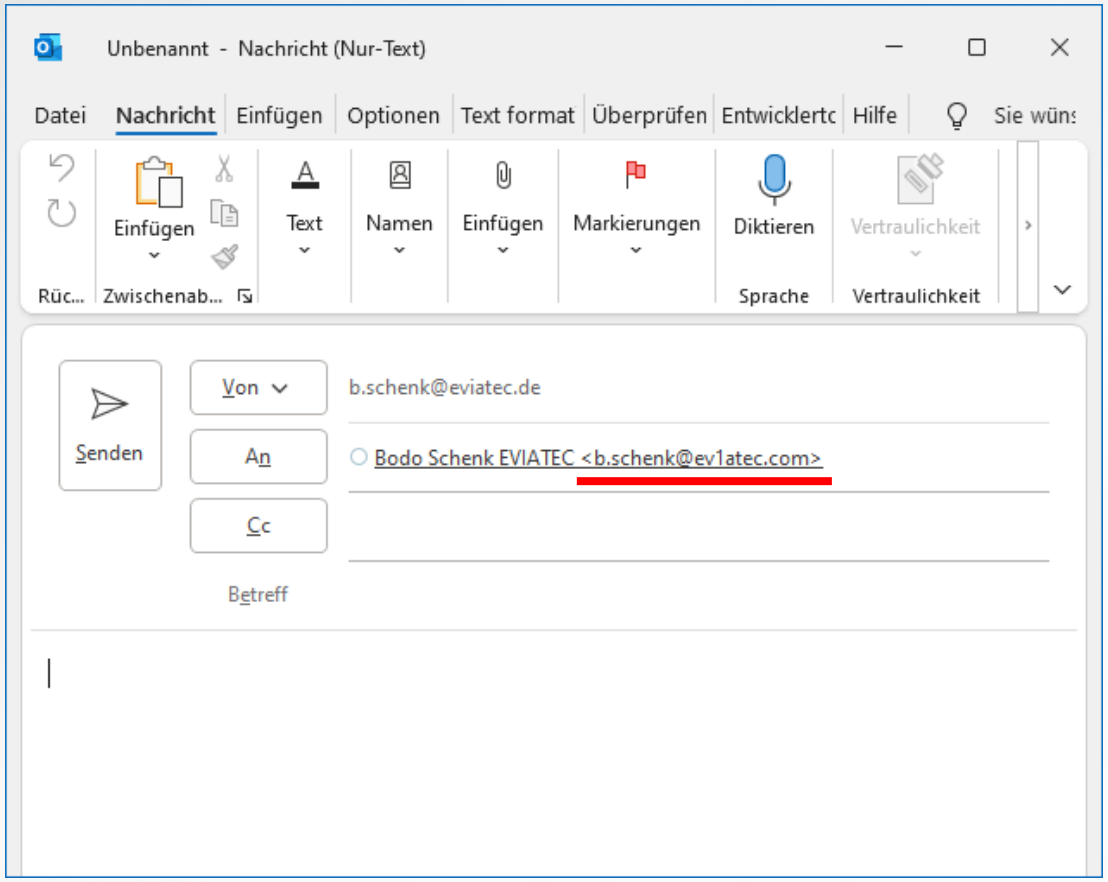
Speichern Sie sich den OWA Link als Favorit und benutzen Sie diesen immer

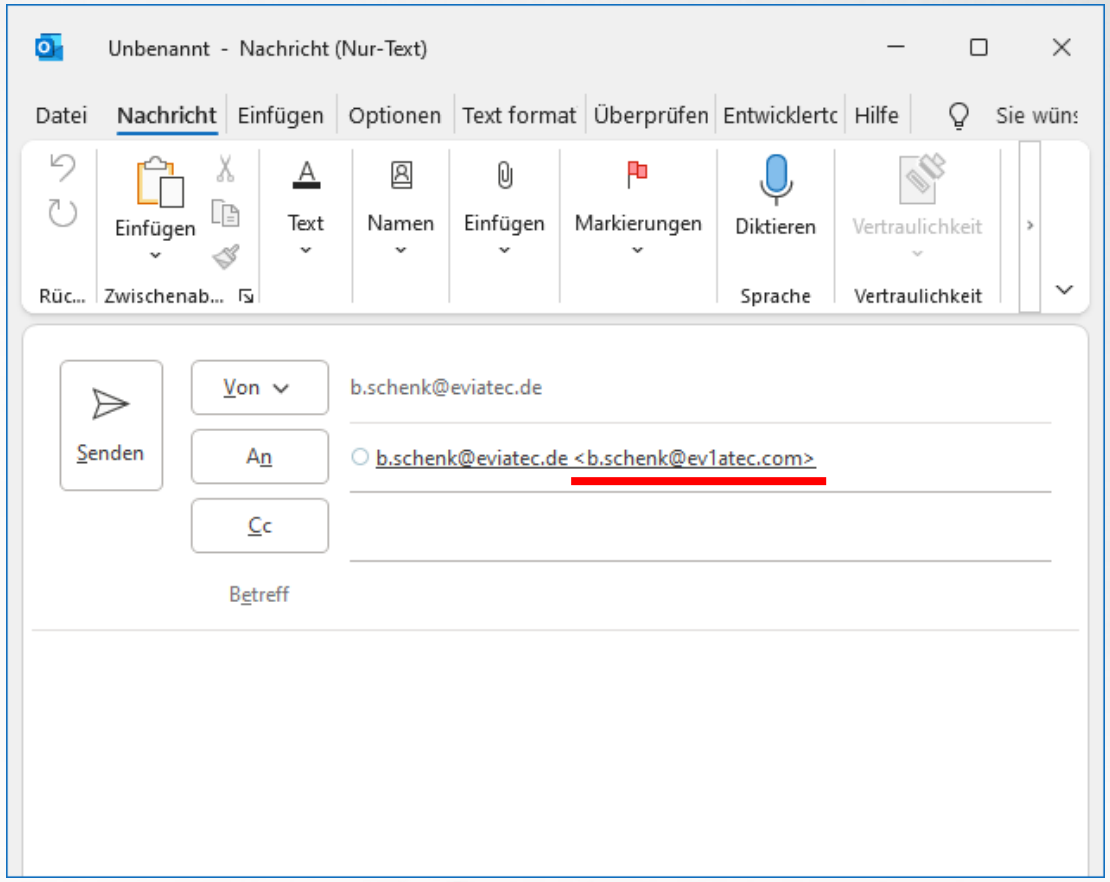
EVIATEC

Prüfen einer Mailadresse

- Prüfen Sie immer, welche Mailadresse angegeben ist
- Fahren Sie mit der Maus über eine Mailadresse, ohne zu klicken
- Die letzten beiden Teile der Mailadresse sind maßgeblich
- Die echte Mailadresse ist i.d.R. in spitzen Klammern angegeben

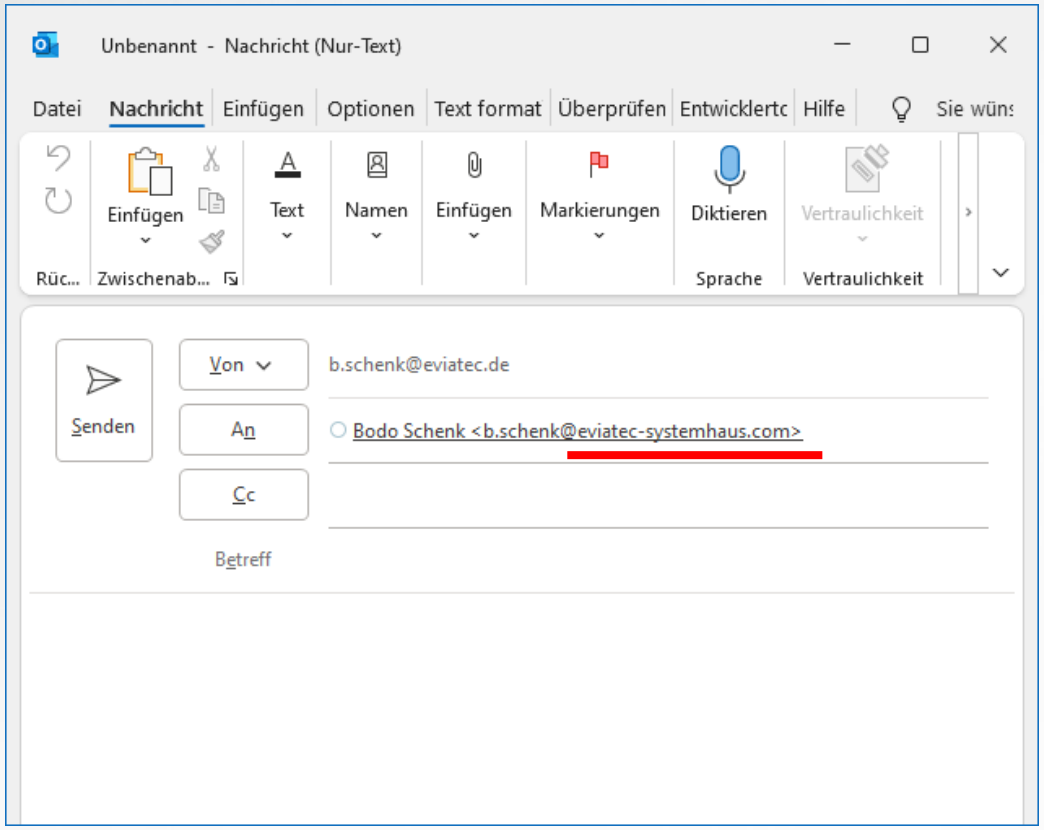
Prüfen einer Mailadresse

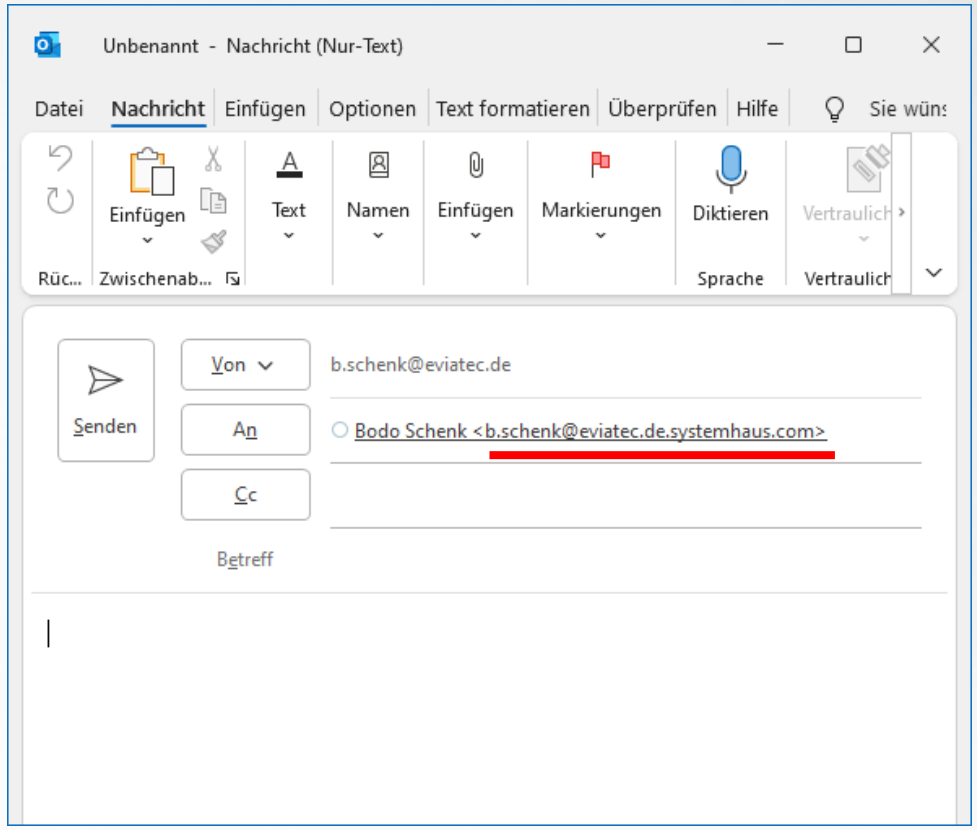




EVIATEC

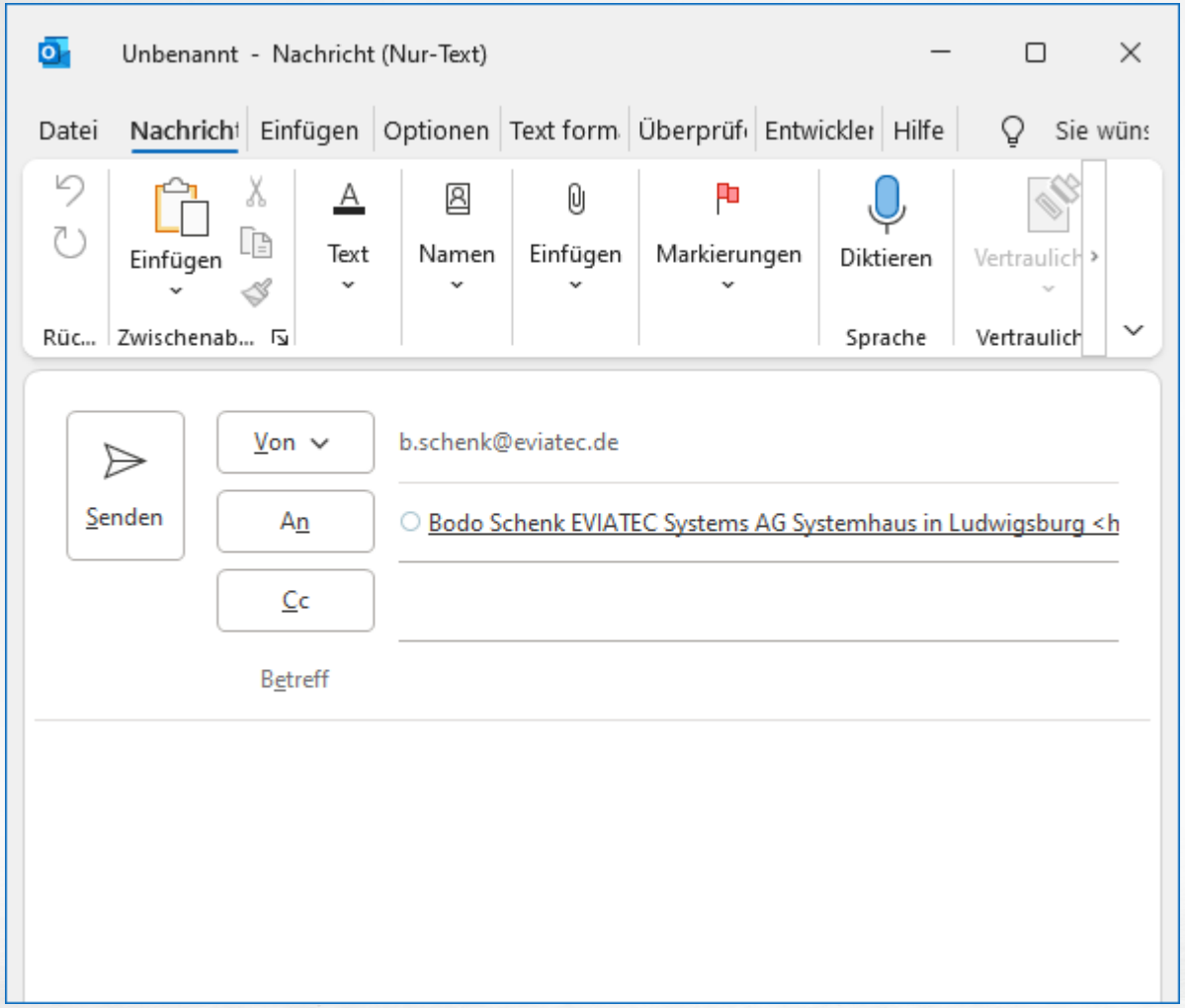
Prüfen einer Mailadresse





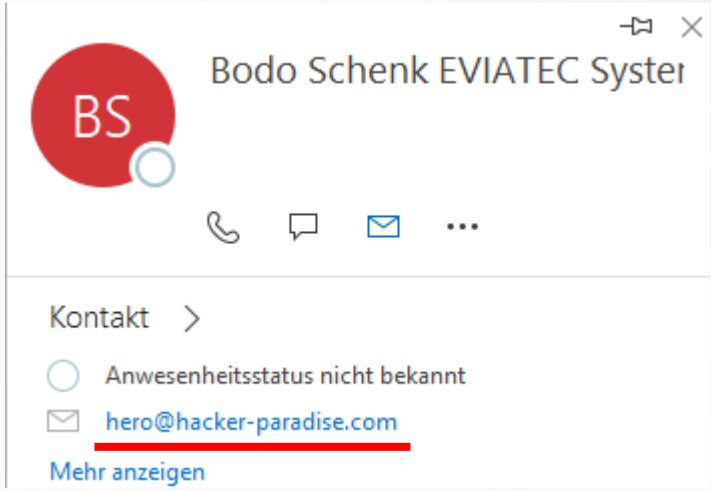
EVIATEC

Prüfen einer Mailadresse



Outlook: wenn man mit der Maus über eine Mailadresse fährt (nicht klicken !) kommen zusätzliche Informationen.

Auch hier ist die gefälschte Adresse zu sehen.



EVIATEC

Dateianhänge

- Direkt ausführbare Dateien - sehr gefährlich
- Makros - gefährlich
- Sonstiges/Read-Only - normalerweise ok
- PDF-Dateien und Bilder i.d.R. ungefährlich
- Prüfen Sie Links innerhalb von PDF Dateien trotzdem wie oben gezeigt

Dateianhänge

Direkt ausführbar

- .exe, .com
- bat, cmd, ps1
- js, vbs
- .wsf, .wsh
- und viele mehr !!!

Makros

- .docm, .dotm
- .xlsm, .xltm
- .pptm, .potm
- und viele mehr !!!
- (.doc, .docx, .dot, .dotx)
- (.xls, .xlsx, .xlt, .xltx)
- (.ppt, .pptx, .pot, .potx)

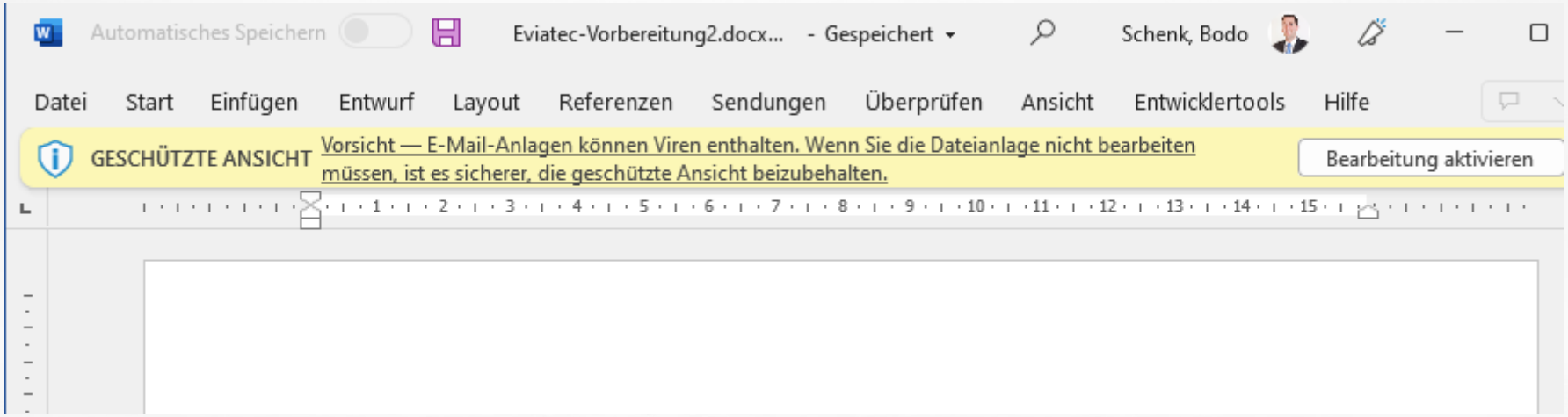
Sonstiges

- PDF
- JPEG, PNG, GIF

Archive: .zip, .7z, .gz, .rar, .tar uvm.

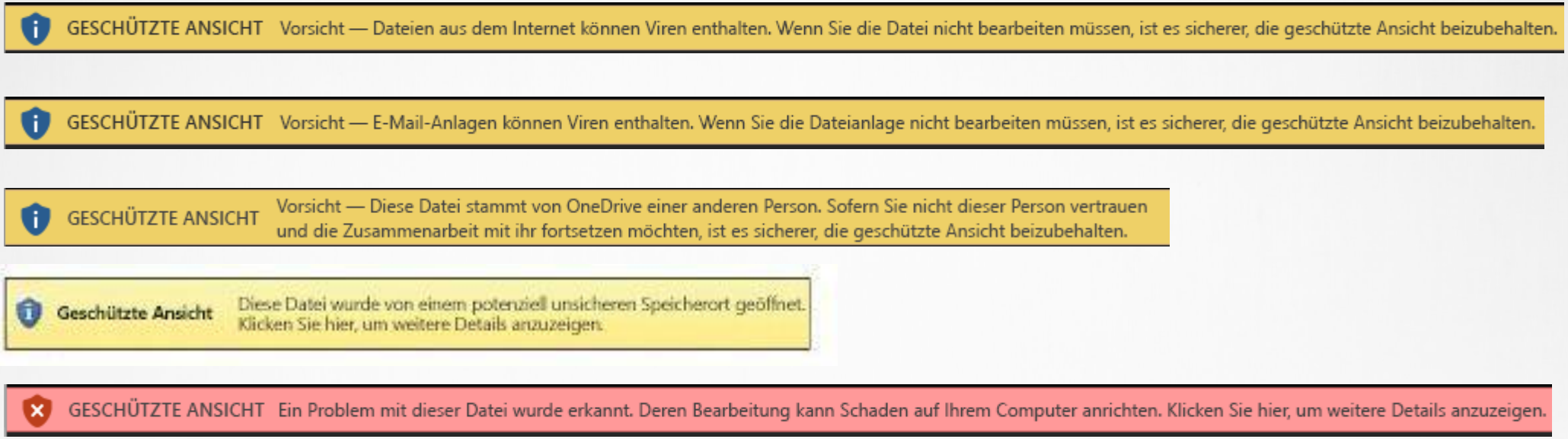
Office: geschützte Ansicht

- Beachten Sie Office Sicherheitsmeldungen zur „geschützten Ansicht“
- Deaktivieren Sie diese Funktion nicht !
- Klicken Sie nicht unvorsichtig auf „Bearbeiten aktivieren“



EVIATEC

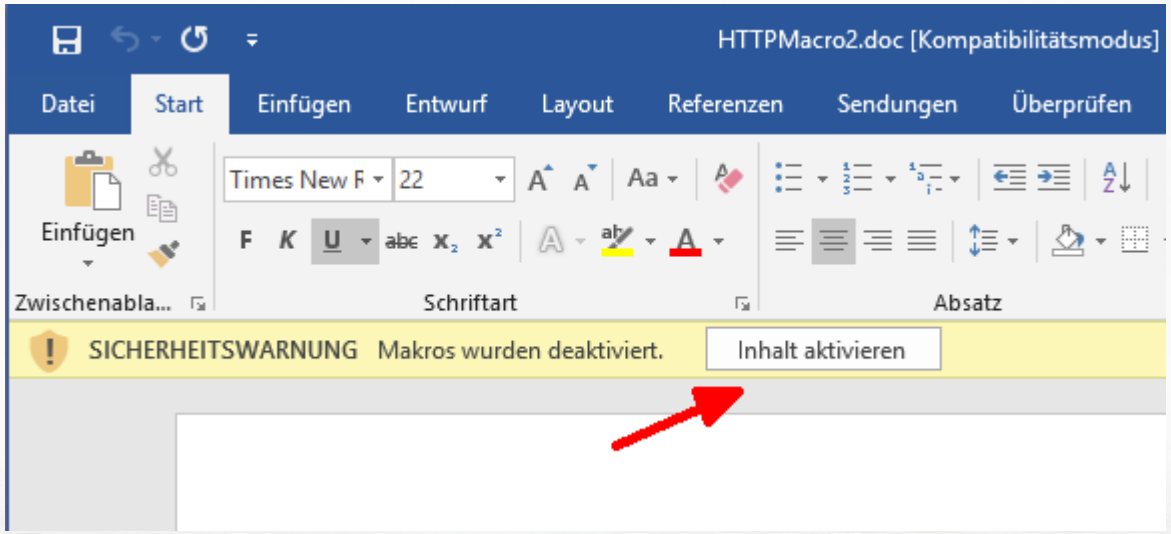
Office: geschützte Ansicht



EVIATEC

Office: Makro Warnungen

- Beachten Sie Office Sicherheitsmeldungen für Makros
- Deaktivieren Sie diese Funktion nicht !
- Klicken Sie nicht unvorsichtig auf „Inhalt aktivieren“



EVIATEC

Im Fall der Fälle

- Und falls Sie doch aus Versehen eine gefährliche Datei gestartet/geöffnet haben ?
- Beispiel: Völlig leeres Word Dokument öffnet sich
- Alle Kabel ziehen (insb. Netzwerkkabel)
- Laptop sofort ausschalten (z.B. Schalter mehrere Sekunden gedrückt halten)
- IT-Abteilung/Sicherheitsabteilung informieren
- Nicht versuchen, den Vorfall auszusitzen („vertuschen“)

Best Practices für private PCs

- Auch Privatpersonen werden angegriffen
- Lösegeldforderungen i.d.R. gering
- Gefahr der Verbreitung HomeOffice -> Arbeit
- Trennen Sie privates und berufliches
  - Nutzen Sie nicht Ihre berufliche Mailadresse als Login für Facebook, Amazon usw.
  - Nutzen Sie nicht Ihre private Mailadresse für berufliche Zwecke
- Social Media (Facebook, Twitter, Instagram, LinkedIn, XING usw.)
  - so wenig Informationen wie möglich teilen
  - wenn, dann nur an Freunde oder geschlossene Gruppen

Best Practices für private PCs

- Halten Sie alle Systeme aktuell
  - Windows
  - Office
  - Virenschutz
  - PDF-Reader usw.
- Die Zeiten, wo man mit Updates „gewartet“ hat, sind vorbei
- Der Schaden einer Infektion ist vielfach höher als der Schaden durch ein fehlgeschlagenes Update

Best Practices für private PCs

- Nutzen Sie zwei verschiedene Accounts
  - Normaler Benutzer für tägliche Arbeit („Bodo“)
  - Admin-User für Installationen („Bodo-ADM“)
  - Unterschiedliche Kennwörter !
- Falls der PC von mehreren Personen genutzt wird, erstellen Sie für jeden einen eigenen Benutzer-Account

Best Practices für private PCs

- Machen Sie regelmäßige Datensicherungen (Backup)
- Mindestens 1x pro Woche
- Bei Backup auf USB-Platte: nach Backup abziehen (Offline)
- Tipp: Veeam Agent für Windows (kostenlos)
- PC/Laptop verschlüsseln (Bitlocker mit StartUp-PIN)
- Nutzen Sie einen professionellen Virenscanner
  - Hochschulangehörige dürfen den TrendMicro Virenscanner auch privat verwenden !
- Firewall, SmartScreen, UAC einschalten

Best Practices für private PCs

- Schalten Sie Sicherheitswarnungen nicht ab, sondern lesen Sie diese
- Misstrauen Sie jeder E-Mail (privat noch mehr als am Arbeitsplatz)
- 2FA wo möglich
  - Schützt vor Passwort-Diebstahl
  - Man wird über einen Missbrauchs-Versuch informiert
- Unterschiedliche Kennwörter bei unterschiedlichen Diensten
  - Trennen privat/geschäftlich
  - Mail, Facebook, Banking, usw.
  - Verwenden Sie Zufallskennwörter mind. 12 Zeichen
  - Verwaltung über ein Password-Safe Tool