Datenschutz und Datensicherheit

SCHULUNGUNTERLAGEN

Übersicht

- Terminologie
- Datenschutz
- Risikobewertungsschema
- Risiken
  - Schadsoftware
  - Phishing
  - Spam
  - Unsichere Hardware
  - Single Sign-On
  - Zugang zu Daten
  - Weitere Gefahren
- Schutzmaßnahmen
  - Verschlüsselte Webseiten
  - Sichere Passwörter
  - Datenlöschung
  - Faktor Mensch
- Aktuelle Themen
- Weiterführende Informationen

Terminologie

Datenschutz	Schutz der Privatsphäre einer Person bzw. der über natürliche Personen gespeicherten Daten.
Datensicherheit	Schutz aller (elektronischen) Daten bzgl. ungewollter Einsichtnahme (Vertraulichkeit) oder Veränderung (Integrität).
Informationssicherheit	Zielt auf einen „ganzheitlichen“ Schutz aller Informationen ab und umfasst somit auch analoge Aufzeichnungen (Aktenaufbewahrung, Abfallentsorgung, etc.).
IT-Sicherheit	Ziele vergleichbar mit Datensicherheit, fokussiert jedoch deutlich stärker Verfügbarkeitsaspekte.

Quelle: https://www.datenschutzbeauftragter-info.de/unterschiede-zwischen-datenschutz-datensicherheit-informationssicherheit-oder-it-sicherheit/

Ziele der Schulung

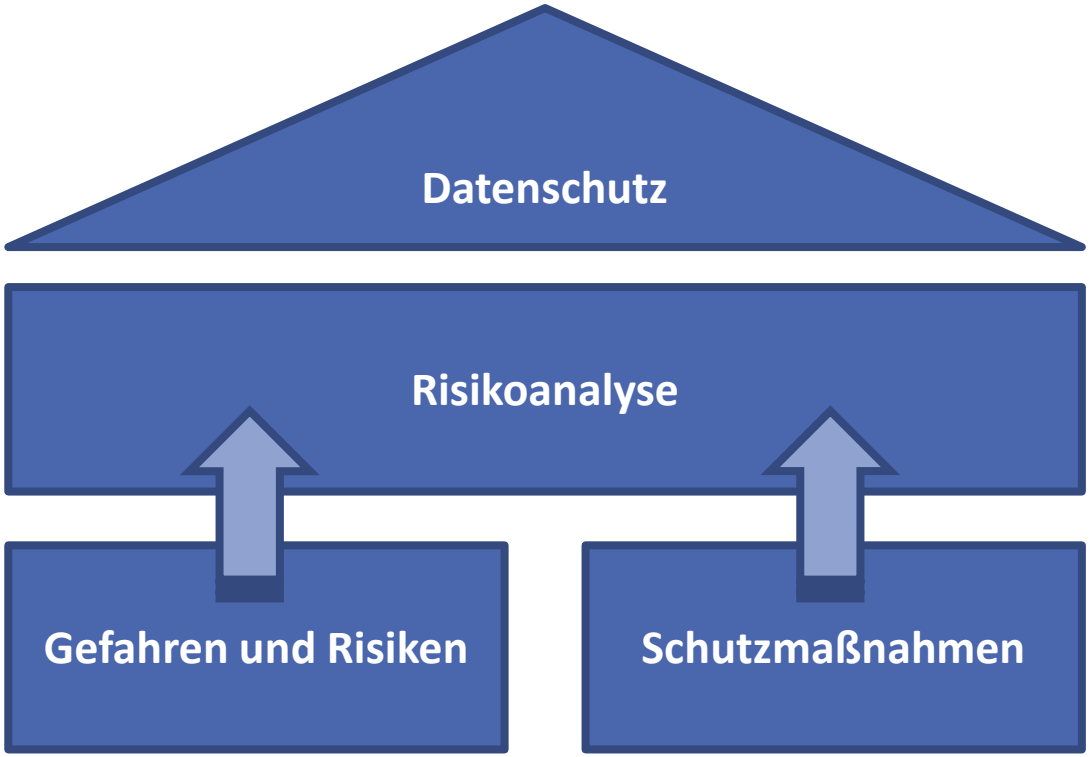
Ziele der Schulung sind:

- Sensibilisierung, um von diesem Thema schon etwas gehört haben.
- Kenntnisse, um mögliche Gefahren früher erkennen zu können.
- Einstieg, um sich neue Denkweisen anzueignen.

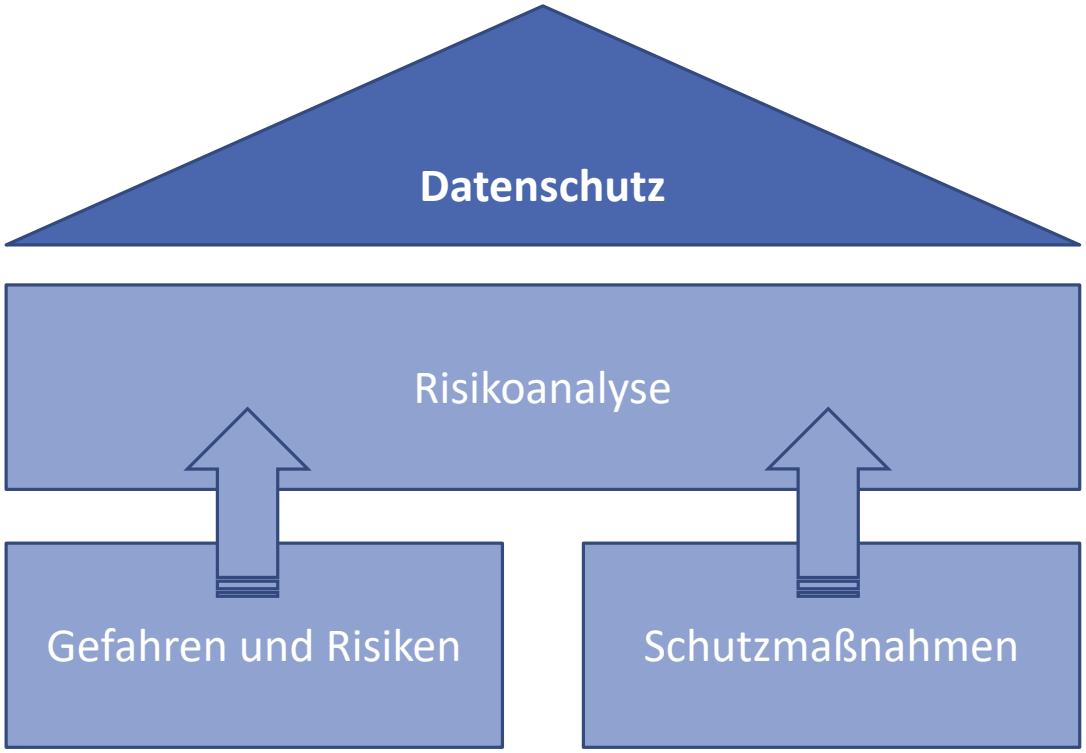
KEINE Ziele sind:

- Alle Arten von Gefahren gezeigt zu bekommen,
- um anschließend selbstständig alle Probleme lösen zu können.

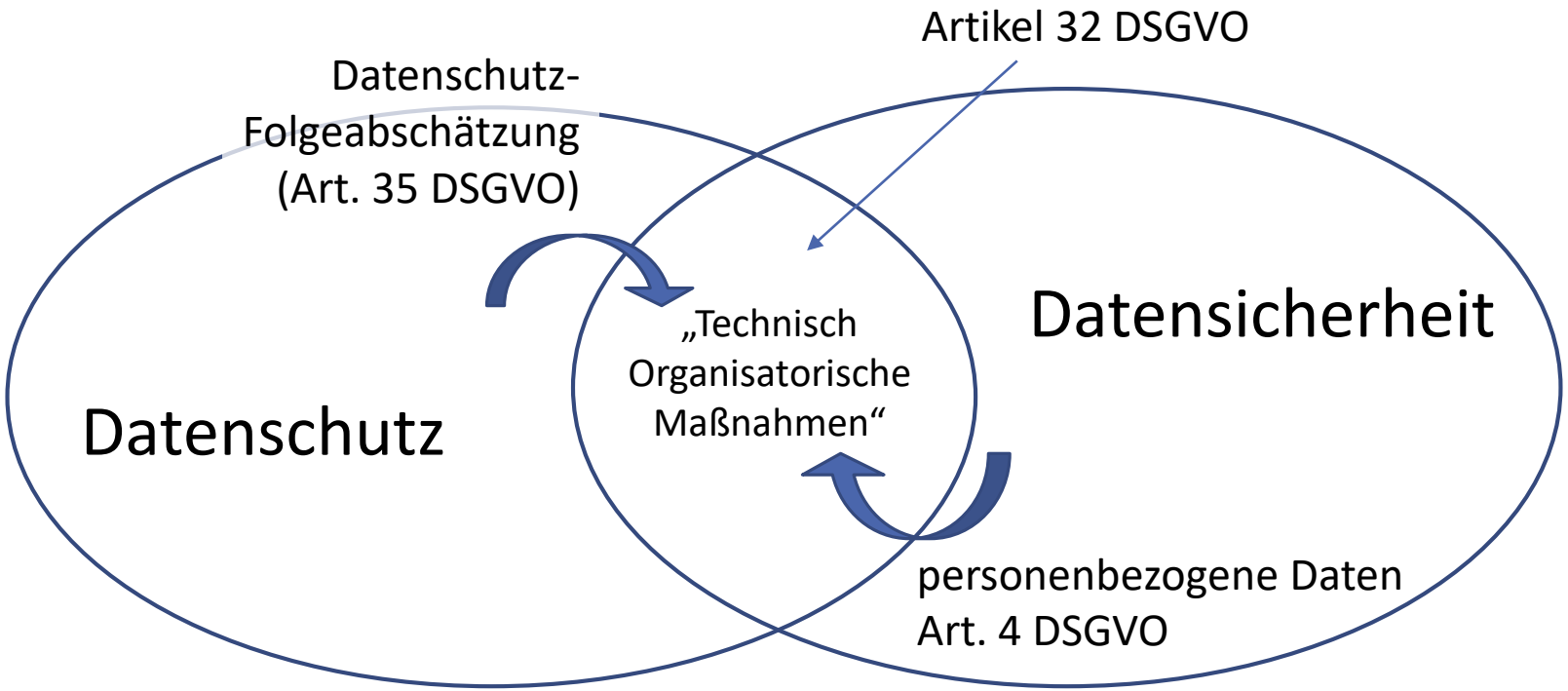
Aufbau der Schulung



Datenschutz



Datenschutz vs. Datensicherheit



Datenschutz (Begriff)

„personenbezogene Daten“:

„personenbezogene Daten“ alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, **die direkt oder indirekt**, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer **Online-Kennung** oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

(Art. 4 DSGVO, eigene Hervorhebungen)

Datenschutz (Datenarten)

Personenbezogene/beziehbare Daten sind:

Name, Geburtsdatum, Alter, Anschrift, E-Mali-Adresse, Telefonnummer, Sozialversicherungsnummer, Steueridentifikationsnummer, Personalausweisnummer, Matrikelnummer, Bankdaten, Online-Daten, physische Merkmale, Besitzmerkmale (z.B. KFZ-Kennzeichen), Werturteile (Zeugnisse), uvm. auch: IP-Adresse

Quelle: https://www.datenschutz.org/personenbezogene-daten/

→ Verarbeitung auf Basis einer Einwilligung oder einer gesetzlichen Grundlage

Datenschutz (Datenarten)

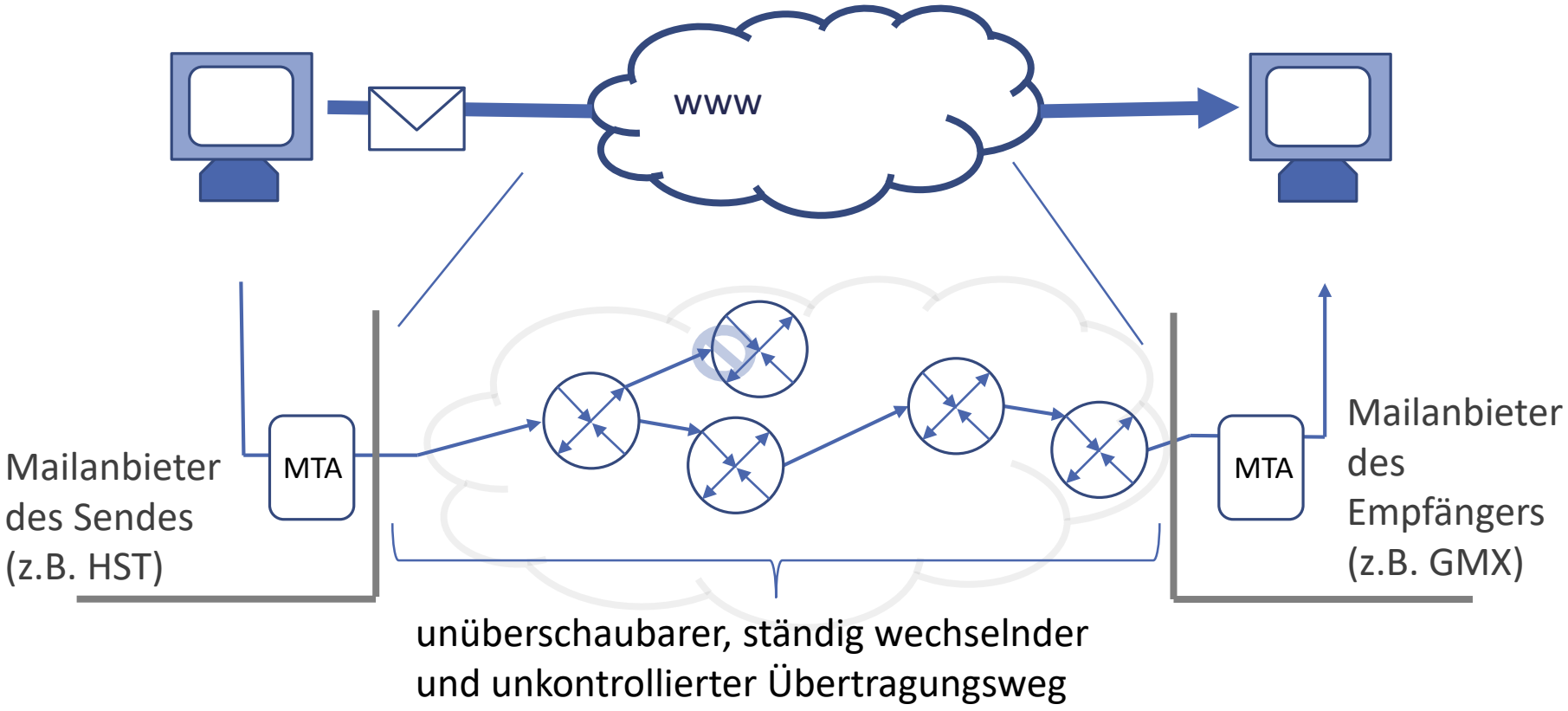
Besonderen Schutz (so genannte „besondere Kategorien“ nach DSGVO):

rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung

(Art. 9 Abs. 1 DSGVO)

→ deutliches Verarbeitungsverbot mit wenigen Ausnahmen

Kontrollverlust (am Bsp. E-Mail)



Risiken (am Bsp. E-Mail)

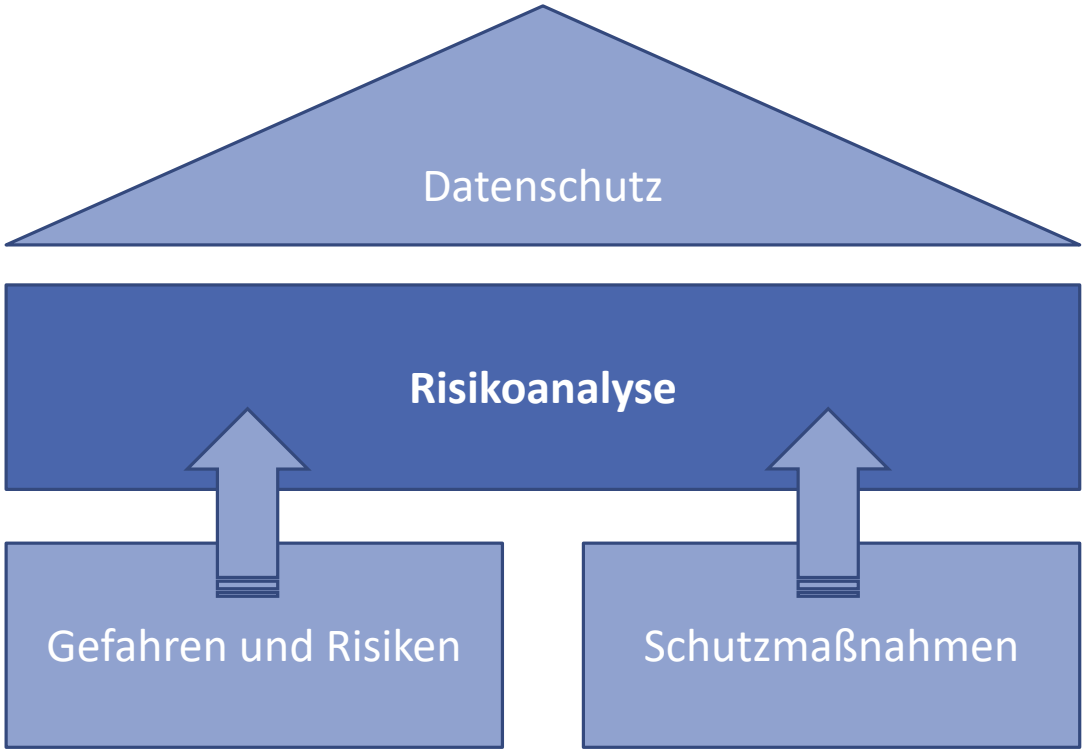
Datenschutz

- Ohne organisatorische Strukturen können datenschutzrechtliche Bestimmungen (Aufbewahrungsfristen, Selbstauskünfte, etc.) nicht eingehalten werden.

Datensicherheit

- Vertraulichkeit nicht sichergestellt: E-Mails selten Ende-zu-Ende verschlüsselt (Ausnahmen: PGP und S/MIME).
- Verarbeitung durch den E-Mail Anbieter möglich (z. B. automatische Verarbeitung durch Googlemail).
- Anhänge in E-Mails immer problematisch (später mehr).

Risikoanalyse



Grundwerte der Informationssicherheit

Vertraulichkeit

Frage nach: „Wer kann das sehen?“

Integrität

Frage nach: „Wer kann das verändern?“

Verfügbarkeit

Frage nach: „Ist das morgen noch da?“

Risikobewertungsschema

Das Schema ermöglicht die Identifikation von potenziellen Risiken und ermöglicht deren Berücksichtigung.

<u>Vertraulichkeit</u> *Wer kann das lesen? Wer hat Zugriff? Was wäre, wenn es morgen jeder wüsste?*	↑ kritisch → neutral ↓ unkritisch
<u>Integrität</u> *Wer kann das ändern? Was passiert, wenn Inhalte falsch sind?*	↑ kritisch → neutral ↓ unkritisch
<u>Verfügbarkeit</u> *Wie lange brauche ich das? Was wäre, wenn es jetzt oder morgen weg ist?*	↑ kritisch → neutral ↓ unkritisch

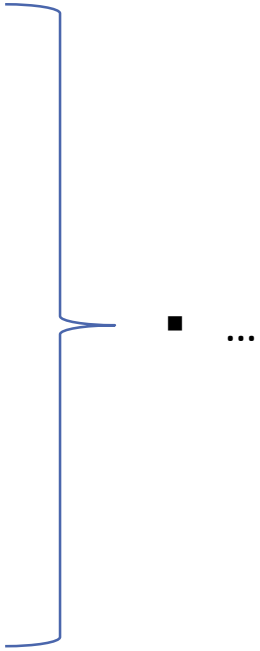
individuelle Einschätzung!

- Ich tue etwas,
- Ich tue etwas nicht,
- Ich überlege mir zusätzliche Maßnahmen um die Sicherheit zu erhöhen

Risikobewertung (Aufgabe)

Versenden einer Liste mit Studierendendaten via E-Mail an eine externe (z.B. @gmx.de) Adresse.

Vertraulichkeit	
Integrität	
Verfügbarkeit	



Schaden abschätzen | Bewerten | Handeln

Risikobewertung (Bsp 1)

Beispiel 1: Versenden einer E-Mail an eine externe Adresse.

Schaden abschätzen	Bewerten	Handeln
Vertraulichkeit *Anbieter (GMX) kann Inhalt lesen. Übertragungsweg ungewiss.*	↑ kritisch	*dazu später mehr* ↓ ▪ E-Mail trotzdem senden ▪ E-Mail nicht senden ▪ Kritische Inhalte zugriffsgeschützt bereitstellen ▪ …
Integrität *Änderung der Daten durch den Anbieter unwahrscheinlich. Änderung der Absenderadresse unwahrscheinlich.*	↓ unkritisch	
Verfügbarkeit *Kopie der Liste noch vorhanden. Unkritisch, wenn die E-Mail nicht ankommt.*	↓ unkritisch	

Risikobewertung (Bsp 2)

Beispiel 2: Verwendung von fremden Speicher- bzw. Clouddiensten (z.B. Dropbox).

Schaden abschätzen	Bewerten	Handeln
Vertraulichkeit *Wer kann die Inhalte lesen? Der Anbieter? Wer hat noch Zugang?*	↑ kritisch	▪ Verzicht auf diese Dienste ▪ Auf unkritische Daten begrenzen ▪ …
Integrität *Was passiert, wenn der Cloudanbieter Änderungen vornimmt?*	→ neutral	
Verfügbarkeit *Was passiert, wenn der Anbieter morgen unangekündigt abschaltet oder den Zugang sperrt?*	→ neutral	

Risikobewertung (Bsp 3)

Beispiel 3: Zutrittssicherung von Büro bzw. der Räumlichkeiten.

Schaden abschätzen	Bewerten	Handeln
Vertraulichkeit *Wer kann den Raum betreten? Welche Informationen sind dort zu finden?*	→ neutral	▪ Lokal gespeicherte Daten minimieren ▪ Nutzung von Speicherdiensten der HST ▪ … ▪ Eigene Backups …? →
Integrität *Haben Änderungen Konsequenzen?*	→ neutral	
Verfügbarkeit *Brand? Wasserschaden? Was wäre, wenn der PC morgen weg ist?*	↑ kritisch	

Risikobewertung (Bsp 4)

Beispiel 4: Backup auf einem USB-Stick.

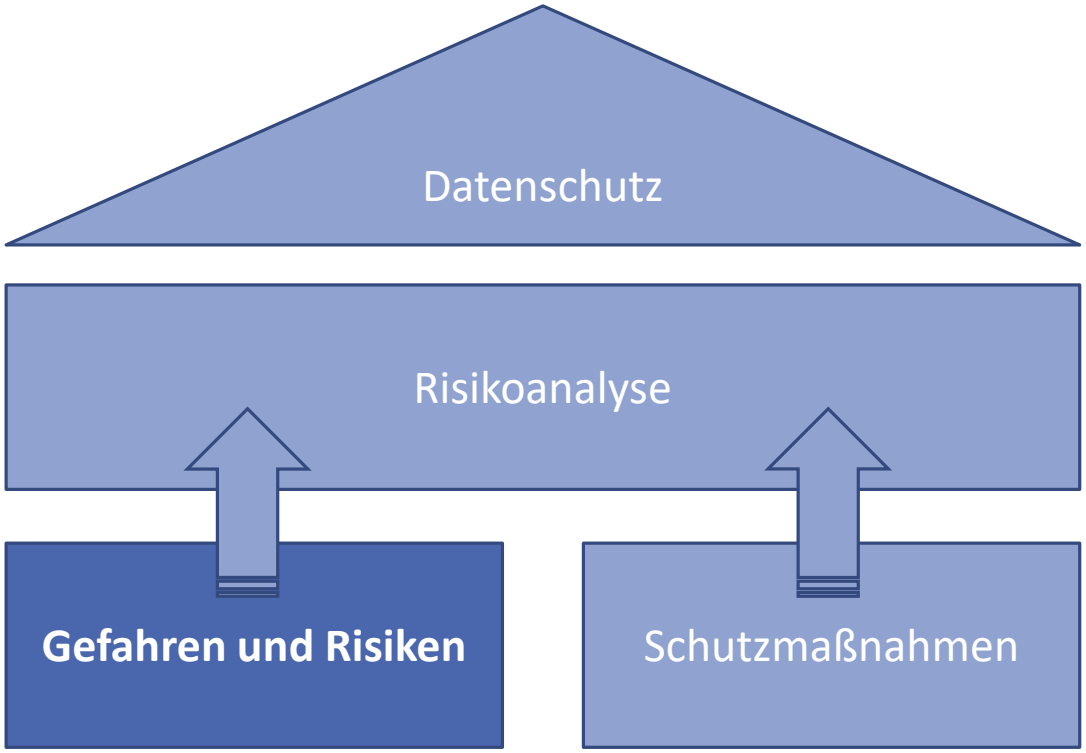
Vertraulichkeit *Was passiert, wenn jemand den Stick klaut? Oder verloren geht?*	↑ kritisch	▪ Backup muss besonders geschützt sein ▪ Verschlüsselung möglich ▪ Regelmäßig Funktionalität prüfen
Integrität *Änderungen am Backup kritisch?*	↓ unkritisch	
Verfügbarkeit *Was ist, wenn der USB-Stick kaputt geht?*	→ neutral	

Schaden abschätzen | Bewerten | Handeln

Probleme und Lösungen

- Lokale Datenablage (wie beschrieben) kritisch: Verlust/Defekt des PCs, Diebstahl, höhere Gewalt, etc.
  → Zentrale Datenablage der Hochschule verwenden (Home-Laufwerk)
- Vertraulichkeitsschutz bei E-Mail Übermittlung ungewiss
  → Bereitstellung „kritischer“ Daten zugriffsgeschützt mit persönlicher Freigabe
    → Seafile mit separater Freigabe: Weitere Infos
    → Alfresco: Weitere Infos
    → Projektgruppenlaufwerke: Weitere Infos
  → Datenübermittlung via E-Mail eher „minimieren“
- Nutzung von USB-Sticks
  → Durch die bereitgestellten Dienste nicht notwendig, kritisch bzgl. Vertraulichkeit und Verfügbarkeit, ggf. nur in Notfällen.

Gefahren und Risiken



Gefahren und Risiken

(1) Schadsoftware: Trojaner und Würmer (*oft via E-Mail)

(2) Schäden durch webbasierte Schadsoftware

(3) Infizierte mobile Apps

(4) Botnetze

(5) Denial-of-Service-Attacken

(6) Spam

(7) Phishing

(8) Viren-Baukästen

(9) Physischer Verlust

(10) Datenverlust

Quelle: Bitkom – Die zehn größten Gefahren im Internet, 27.03.2015

ROT: Faktor Mensch involviert

Schadsoftware (Überblick)

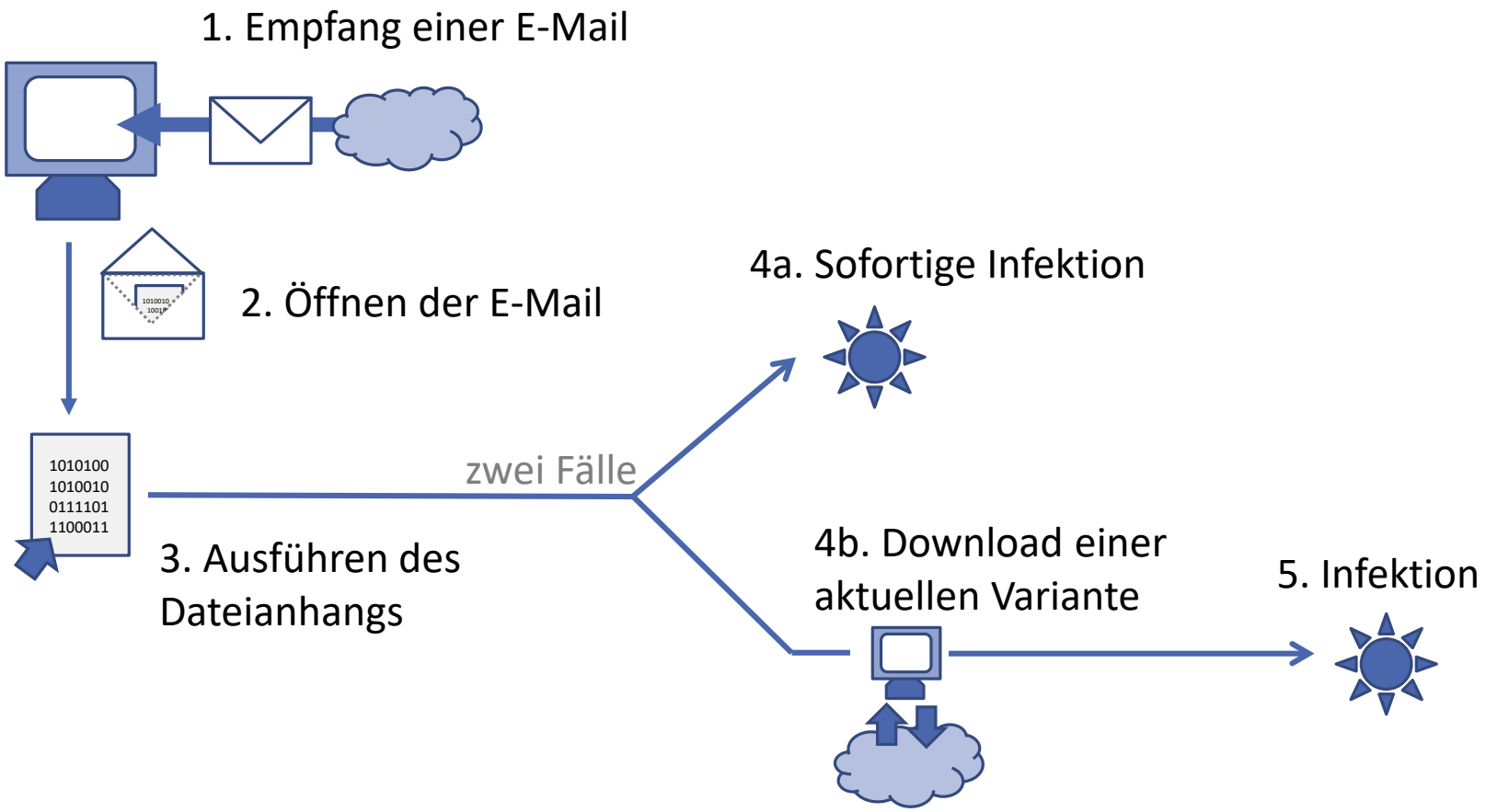
- Verschiedene Arten von Schadsoftware; „Virus“ nur eine Gruppe davon und tritt nur noch selten in Erscheinung
- Überwiegend (zunächst) unentdeckt (außer Spyware)
- Ziele:
  - Abgriff von „kritischen“ Daten, z.B. Passwörter für Identitätsdiebstahl
  - Nutzung der Hardware für fremde Zwecke (Botnetze, Spam E-Mails)
  - „Gefangennahme“ der Daten zu Erpressungszwecken
  - Neuerdings auch: „Bitcoin“-Mining
- Angriffsvektoren (Infektionswege):
  - E-Mail Anhänge mit ausführbarem Inhalt
  - Unseriöse Anwendungen oder „Drive-by-Download“ Exploit bei kompromittierten Webseiten und begünstigt durch veraltete Browser
  - Exploit bei Servern bei Einsatz verwundbarer Software

…

Schadsoftware (Schutz)

- Schutz durch
  - Vorsicht
    Zurückhaltung bei ausführbaren Anwendungen – insbesondere sollten Dateianhänge bei E-Mail sehr kritisch untersucht werden.
  - Softwareupdates
    Betrifft sowohl Betriebssystem, als auch die installierten Anwendungen. Falls die Pflege zu viel Aufwand verursacht sollte ungenutzte Programme deinstalliert werden.
  - Virenscanner
    Der Schutzwirkung von Virenscannern wird allgemein überschätzt. Überwiegend Schutz vor Infektion, wenig Wirkung bzgl. nachträglicher Bereinigung.

Schadsoftware (via E-Mail)

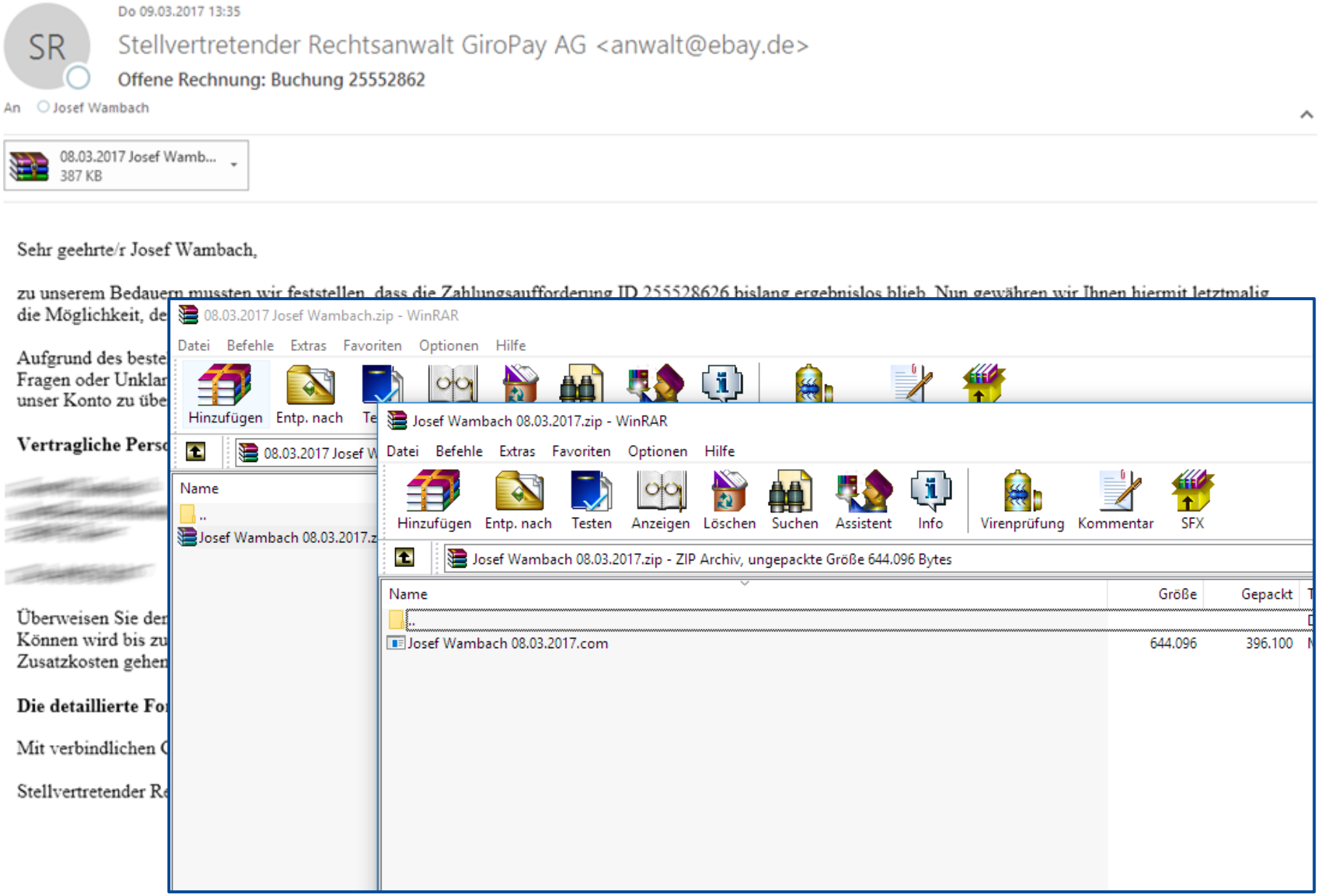


Schadsoftware (Tarnung)

- Häufiger Fall: Dateianhang ist eine ausführbare Datei, die sich ggf. als „Dokument“ tarnt:
  - .pdf.exe als Dateiendung, auch möglich: .pdf.com (.exe, .com, .bat. sind potenziell gefährlich)
  - Icon (Bild) der Datei wirkt wie Nutzdaten (z.B. PDF), ist jedoch ausführbar
- Ebenfalls vorkommend:
  - Versteckte Skripte in Word/Excel (Makros)
  - Schwachstelle in Applikationen (z.B Acrobat Reader)
  - Schadsoftware in legitimen Anwendungen aus unseriösen Quellen
- Selbstverbreitend
  - Schwachstellen die über das Netzwerk ausgenutzt werden können.

Trojaner

Würmer


Do 09.03.2017 13:35
SR
Stellvertretender Rechtsanwalt GiroPay AG <anwalt@ebay.de>
Offene Rechnung: Buchung 25552862
An Josef Wambach
08.03.2017 Josef Wamb...
387 KB
Sehr geehrte/r Josef Wambach,
zu unserem Bedauern mussten wir feststellen, dass die Zahlungsaufforderung ID 255528626 bislang ergebnislos blieb. Nun gewähren wir Ihnen hiermit letztmalig
die Möglichkeit, de
Aufgrund des beste
Fragen oder Unklar
unser Konto zu übe
Vertragliche Pers
Überweisen Sie der
Können wird bis zu
Zusatzkosten gehen
Die detaillierte Fo
Mit verbindlichen G
Stellvertretender Re
08.03.2017 Josef Wambach.zip - WinRAR
Datei Befehle Extras Favoriten Optionen Hilfe
Hinzufügen Entp. nach
Josef Wambach 08.03.2017.zip - WinRAR
Datei Befehle Extras Favoriten Optionen Hilfe
Hinzufügen Entp. nach Testen Anzeigen Löschen Suchen Assistent Info Virenprüfung Kommentar SFX
Josef Wambach 08.03.2017.zip - ZIP Archiv, ungepackte Größe 644.096 Bytes
Name
Größe
Gepackt
Josef Wambach 08.03.2017.com
644.096
396.100

Schadsoftware (Umgang)

Vorher

- Kollegen fragen
- gerne HST Rechenzentrum fragen
- im Zweifel besser vorsichtig sein
- … eher misstrauisch sein

Nachher (bzw. im Ernstfall)

I. Ruhe bewahren

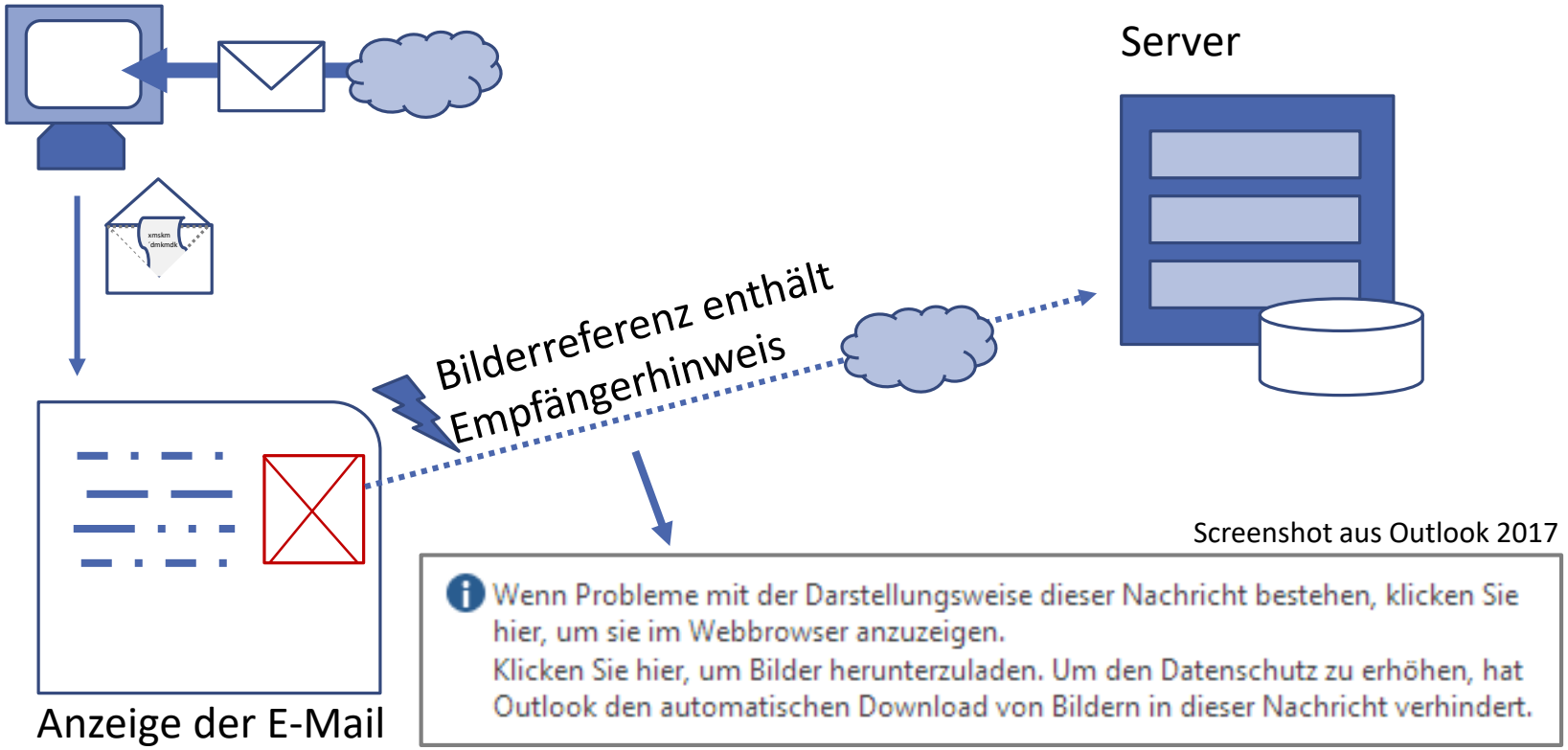
II. Bei PC: Trennung vom Netzwerk immer sinnvoll

III. HST anrufen und fragen, falls unerreichbar: PC ausschalten

Spam

- Name entstammt vom Dosenfleisch SPAM (Spiced Pork and Ham); auch bekannt durch Monty Python Sketch (Spam-Sketch).
- Überbegriff für unerwünschte E-Mail:
  - Scam: Dubiose Job/Geld Angebote
  - Hoax: Schwindel/Schlechter Scherz (“Kettenbriefe”)
  - Phishing: Social Engineering (wird separat behandelt)
- Empfängeradressen werden (häufig) durch Absuchen von Webseiten gesammelt.
- Verursachter wirtschaftlicher Schaden wird höher als durch Autodiebstähle (Quelle: BSI) geschätzt.

Spam (Bilder in E-Mails)



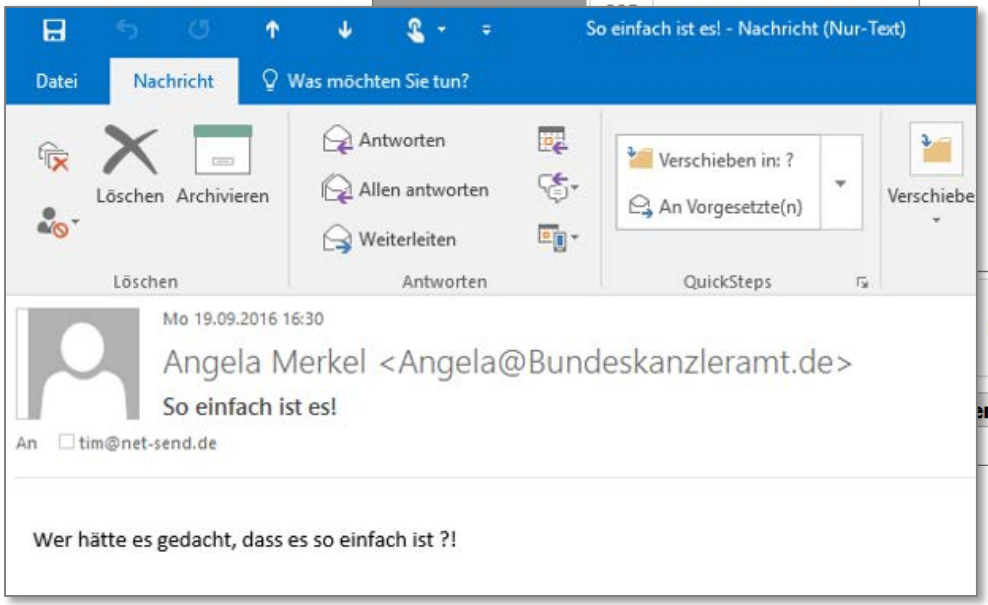
Bei Spam sollte das Nachladen von Bildern vermieden werden.

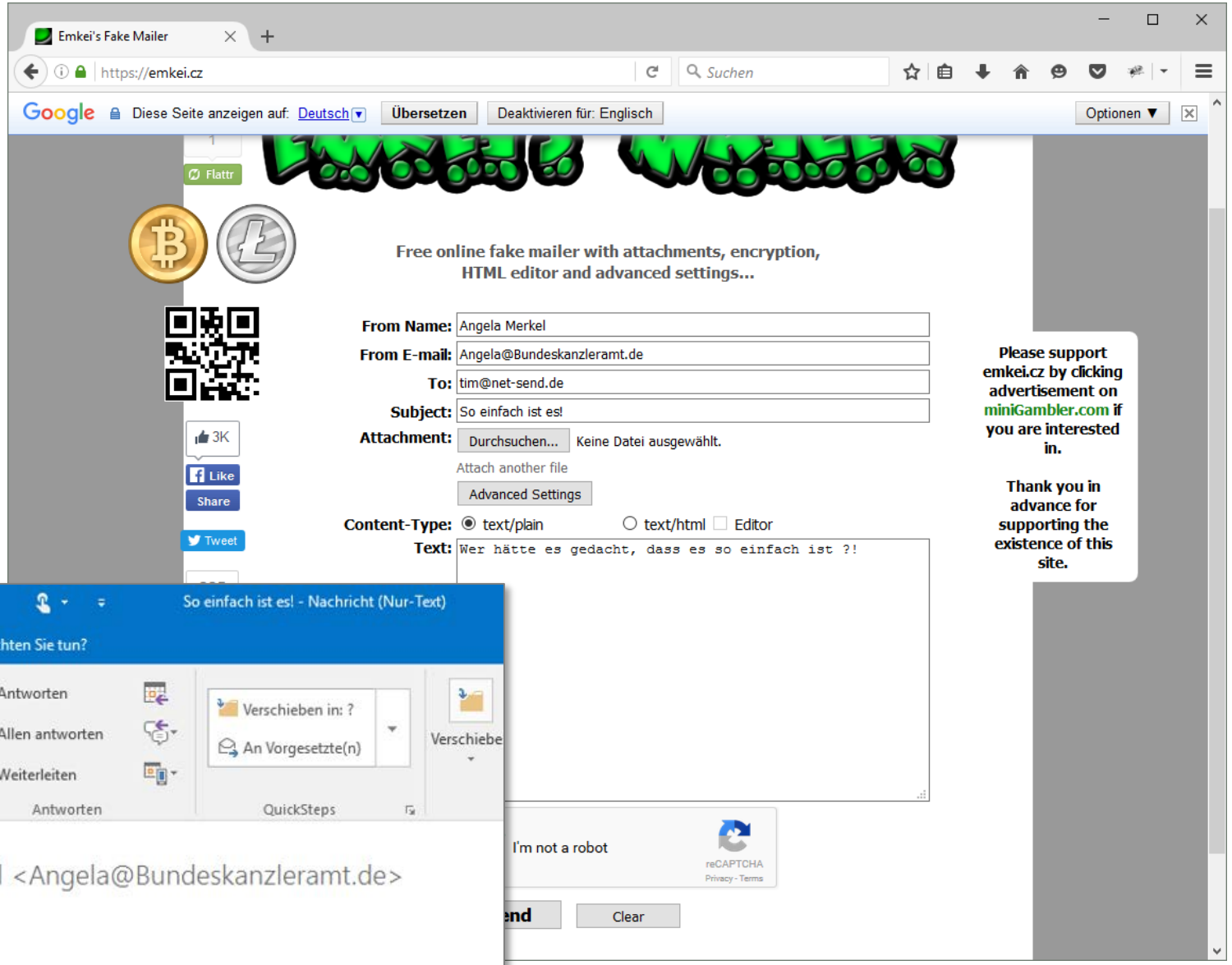
Phishing

- Englisches Kunstwort, das an fishing (angeln, fischen) angelehnt ist.
- Ziel ist der Identitätsdiebstahl: Passwörter, PINs/TANs, Kreditkarteninformationen, etc.
- Gruppe der Social Engineering Angriffe (Mensch als Schwachstelle).
- E-Mail oder Messenger (auch SMS) als Verbreitungsweg.
- …

Phishing (Funktionsweise)

- Absender von E-Mails können leicht gefälscht werden.
  - Merke: Er ist exakt genau so sicher, wie der Absender auf einem Briefumschlag
  - E-Mails mit gefälschtem Absender deuten nicht automatisch auf eine Schadsoftwareinfektion hin.
- Die Gestaltung einer E-Mail kann leicht von echten kopiert werden.
- Allgemein bei Social Engineering: Ausnahmesituationen oder Konfliktsituationen werden ausgenutzt.
- (Hyper)Links in E-Mails können anders reagieren als erwartet.
  - Beispiel 1: http://www.spiegel.de/

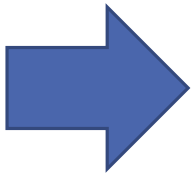




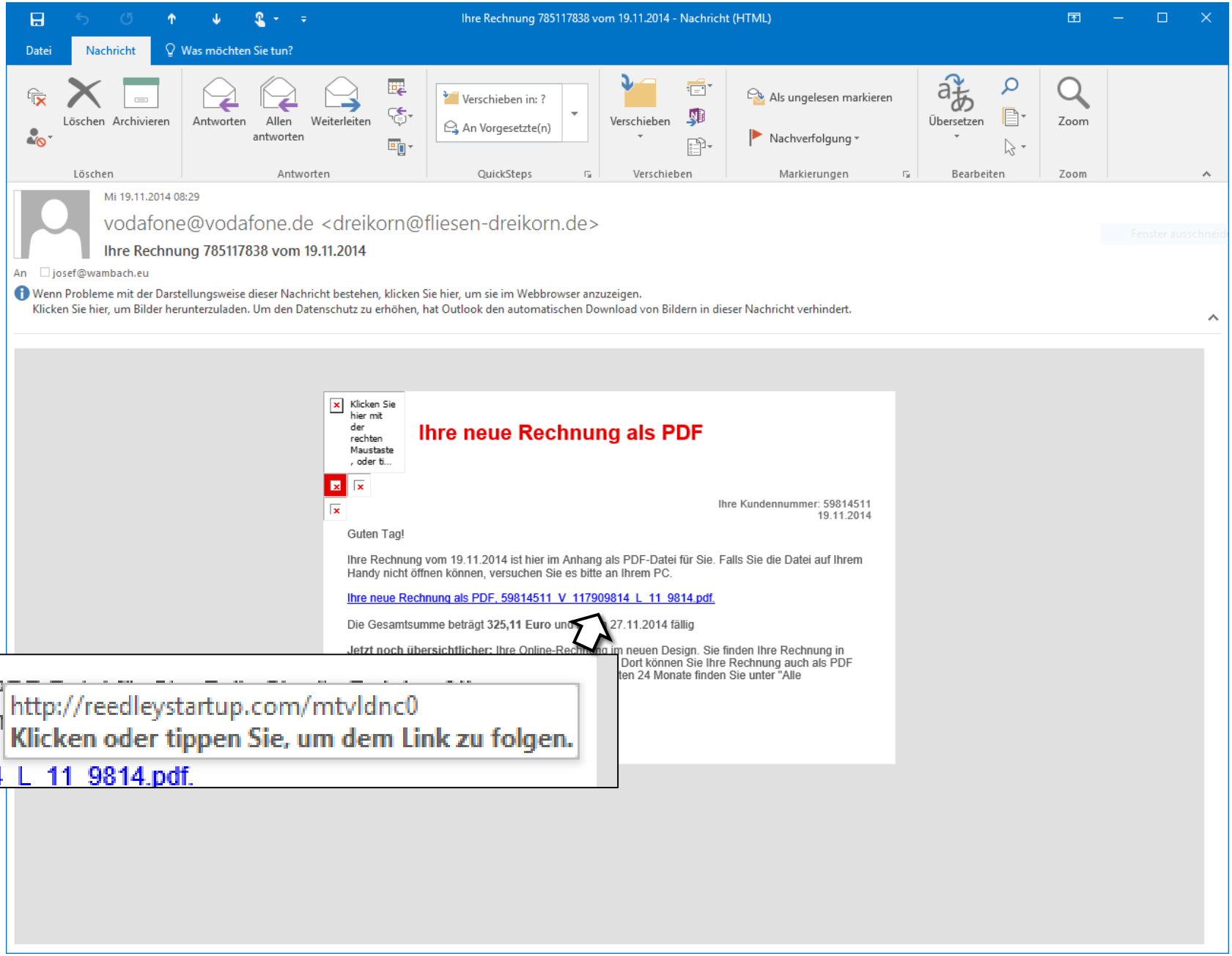
Nutzung wird ausdrücklich nicht empfohlen!

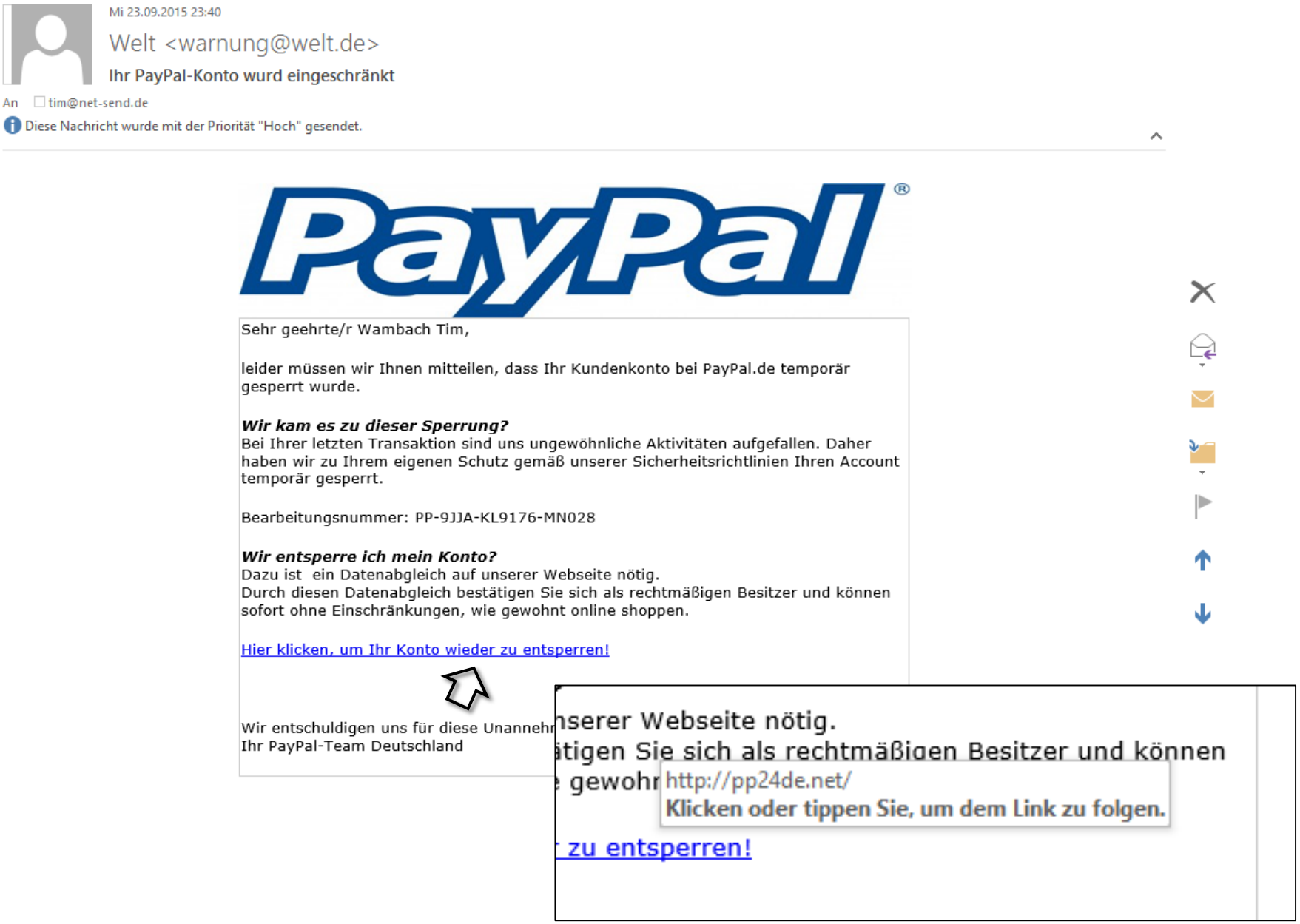
Phishing (Hinweise)

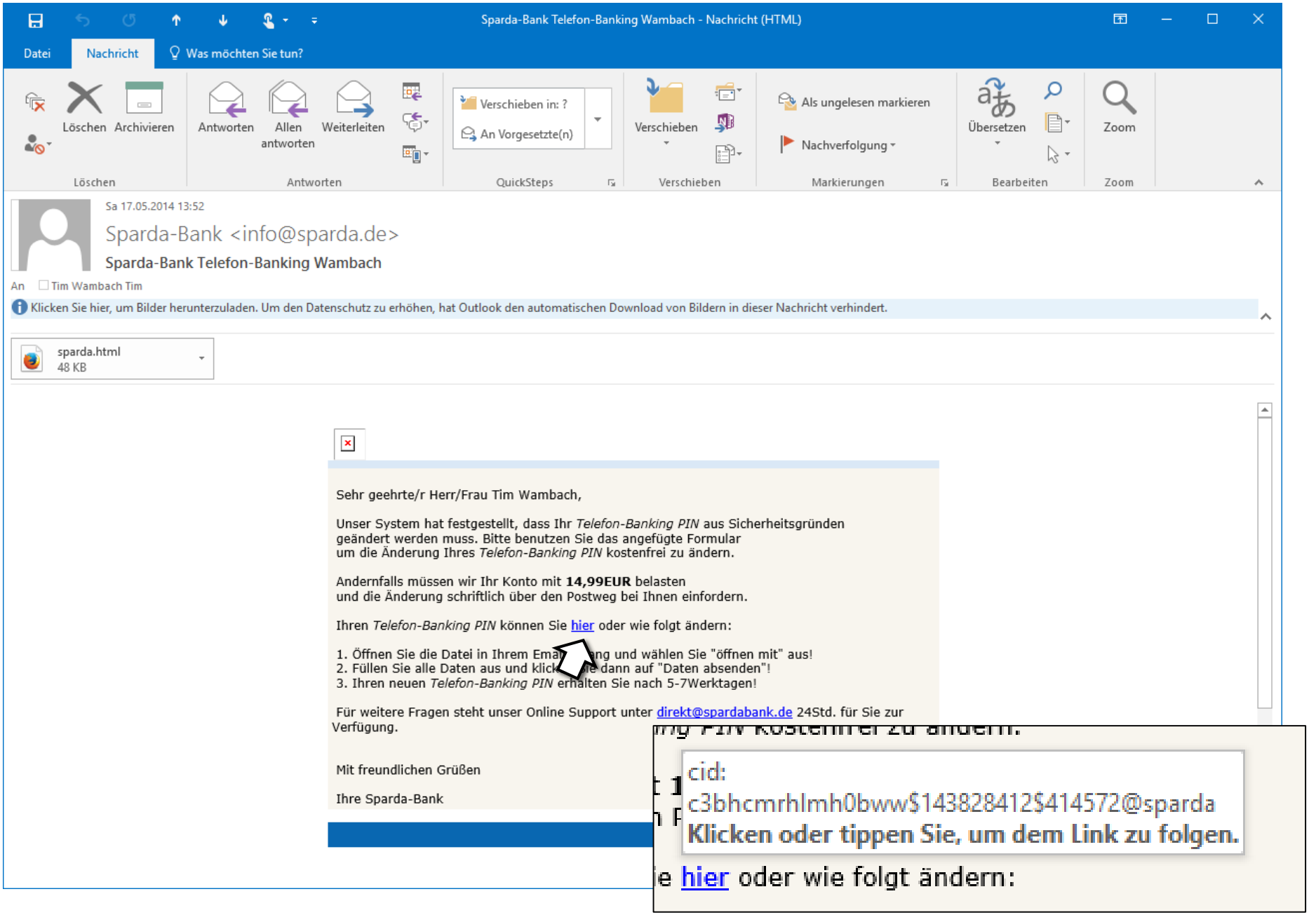
- Grammatik und Orthographie-Fehler
- Text in fremder Sprache
  (Probleme bei Umlauten!)
- Fehlender Name
- Dringender Handlungsbedarf,
  Drohungen
- Aufforderung zur Eingabe von Daten
- Aufforderung zur Öffnung einer Datei
- Links oder eingefügte Formulare
- Kein Kunde



Beispiele


Ihre Rechnung 785117838 vom 19.11.2014 - Nachricht (HTML)
Datei
Nachricht
Was möchten Sie tun?
Löschen
Archivieren
Antworten
Allen antworten
Weiterleiten
Verschieben in: ?
An Vorgesetzte(n)
Verschieben
Als ungelesen markieren
Nachverfolgung
Übersetzen
Zoom
Löschen
Antworten
QuickSteps
Verschieben
Markierungen
Bearbeiten
Zoom
Mi 19.11.2014 08:29
vodafone@vodafone.de <dreikorn@fliesen-dreikorn.de>
Ihre Rechnung 785117838 vom 19.11.2014
An josef@wambach.eu
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.
Klicken Sie hier mit der rechten Maustaste , oder ti...
Ihre neue Rechnung als PDF
Ihre Kundennummer: 59814511
19.11.2014
Guten Tag!
Ihre Rechnung vom 19.11.2014 ist hier im Anhang als PDF-Datei für Sie. Falls Sie die Datei auf Ihrem Handy nicht öffnen können, versuchen Sie es bitte an Ihrem PC.
Ihre neue Rechnung als PDF, 59814511_V_117909814_L_11_9814.pdf.
Die Gesamtsumme beträgt 325,11 Euro und
27.11.2014 fällig
Jetzt noch übersichtlicher: Ihre Online-Rechnung im neuen Design. Sie finden Ihre Rechnung in
Dort können Sie Ihre Rechnung auch als PDF
ten 24 Monate finden Sie unter "Alle
http://reedleystartup.com/mtvldnc0
Klicken oder tippen Sie, um dem Link zu folgen.
4_L_11_9814.pdf.


Mi 23.09.2015 23:40
Welt <warnung@welt.de>
Ihr PayPal-Konto wurd eingeschränkt
An tim@net-send.de
Diese Nachricht wurde mit der Priorität "Hoch" gesendet.
PayPal
Sehr geehrte/r Wambach Tim,
leider müssen wir Ihnen mitteilen, dass Ihr Kundenkonto bei PayPal.de temporär gesperrt wurde.
Wir kam es zu dieser Sperrung?
Bei Ihrer letzten Transaktion sind uns ungewöhnliche Aktivitäten aufgefallen. Daher haben wir zu Ihrem eigenen Schutz gemäß unserer Sicherheitsrichtlinien Ihren Account temporär gesperrt.
Bearbeitungsnummer: PP-9JJA-KL9176-MN028
Wir entsperre ich mein Konto?
Dazu ist ein Datenabgleich auf unserer Webseite nötig.
Durch diesen Datenabgleich bestätigen Sie sich als rechtmäßigen Besitzer und können sofort ohne Einschränkungen, wie gewohnt online shoppen.
Hier klicken, um Ihr Konto wieder zu entsperren!
Wir entschuldigen uns für diese Unannehr
Ihr PayPal-Team Deutschland
nserer Webseite nötig.
ätigen Sie sich als rechtmäßigen Besitzer und können
gewohr
http://pp24de.net/
Klicken oder tippen Sie, um dem Link zu folgen.
zu entsperren!


Sparda-Bank Telefon-Banking Wambach - Nachricht (HTML)
Datei
Nachricht
Was möchten Sie tun?
Löschen
Archivieren
Antworten
Allen antworten
Weiterleiten
Verschieben in: ?
An Vorgesetzte(n)
Verschieben
Als ungelesen markieren
Nachverfolgung
Übersetzen
Zoom
Löschen
Antworten
QuickSteps
Verschieben
Markierungen
Bearbeiten
Zoom
Sa 17.05.2014 13:52
Sparda-Bank <info@sparda.de>
Sparda-Bank Telefon-Banking Wambach
An Tim Wambach Tim
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.
sparda.html
48 KB
Sehr geehrte/r Herr/Frau Tim Wambach,
Unser System hat festgestellt, dass Ihr Telefon-Banking PIN aus Sicherheitsgründen geändert werden muss. Bitte benutzen Sie das angefügte Formular um die Änderung Ihres Telefon-Banking PIN kostenfrei zu ändern.
Andernfalls müssen wir Ihr Konto mit 14,99EUR belasten und die Änderung schriftlich über den Postweg bei Ihnen einfordern.
Ihren Telefon-Banking PIN können Sie hier oder wie folgt ändern:
1. Öffnen Sie die Datei in Ihrem Ema ng und wählen Sie "öffnen mit" aus!
2. Füllen Sie alle Daten aus und klick e dann auf "Daten absenden"!
3. Ihren neuen Telefon-Banking PIN erhalten Sie nach 5-7Werktagen!
Für weitere Fragen steht unser Online Support unter direkt@spardabank.de 24Std. für Sie zur Verfügung.
Mit freundlichen Grüßen
Ihre Sparda-Bank
cid:
c3bhcmrhlmh0bww$14382812$414572@sparda
Klicken oder tippen Sie, um dem Link zu folgen.
e hier oder wie folgt ändern:

Unsichere Hardware

Auch „einfache“ Hardware wie Drucker, Scanner, Beamer etc. bietet häufig mehr Angriffsfläche als auf den ersten Blick sichtbar.

Pearl.de , am 10.10.2017

Was der Anwender sieht:

WLAN-Verbindung: Einfach und schnell verbinden Sie den Drucker mit Netzwerk, PCs und Mobilgeräten mit **Android und iOS!** So greifen Sie **ganz ohne Kabelsalat** auf alle Funktionen zu, auch aus verschiedenen Räumen. Dank **AirPrint-Kompatibilität** drucken Sie Ihre Aufträge ohne zusätzliche Treiber direkt von Ihrem Apple-Gerät! Mit an Bord ist auch **Wi-Fi Direct:** Verbinden Sie bis zu 8 Nutzer direkt mit Ihrem Drucker. So scannen und drucken Sie auch ohne vorhandenes WLAN-Netzwerk.

Was der Techniker sieht:

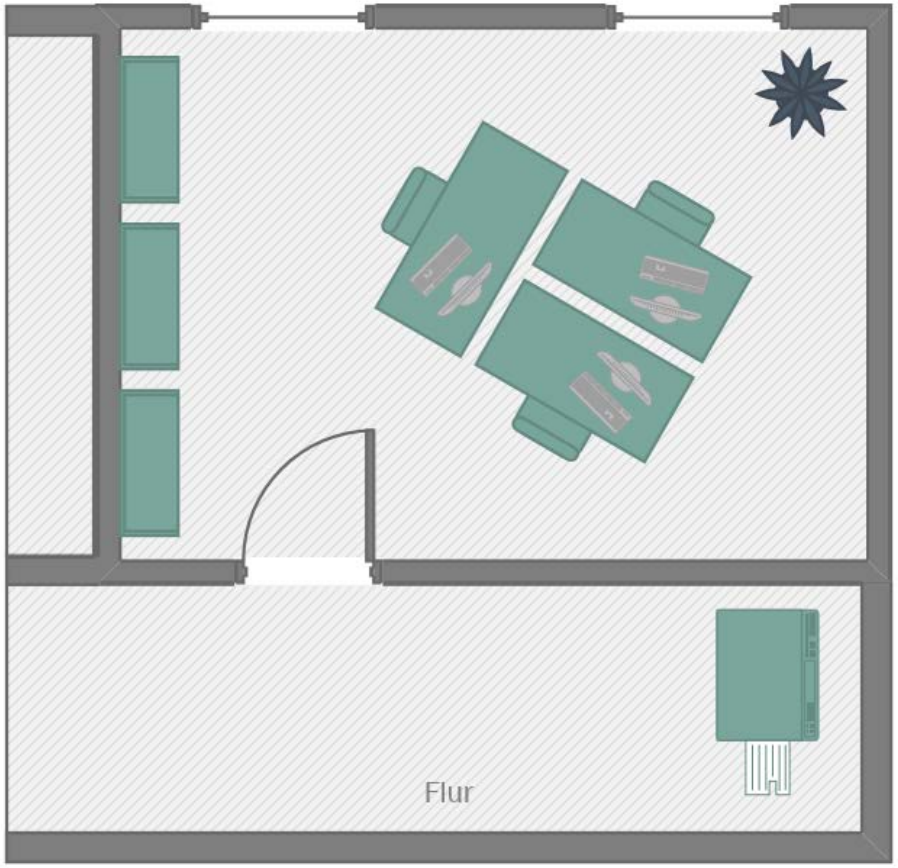
- Eigener WLan Accesspoint (Störquelle)
- Zugriff auf Webinterface mit Standardpasswörtern
- Abgreifen von Druckaufträgen und Scans
- Möglicher ungeschützter Netzübergang

Single Sign-On

- Beispiel: Shibboleth
- Vorteile
  - nur ein Zugang (und ein Passwort) für mehrere Dienste
  - Zugang zu Diensten bei anderen unterstützenden Institutionen
- Nachteil
  - Kein Single Sign-Out möglich, Abmeldung wird erst durch ein Timeout bewirkt.
  - Weitergabe von Benutzerdaten (Datenschutzaspekte).

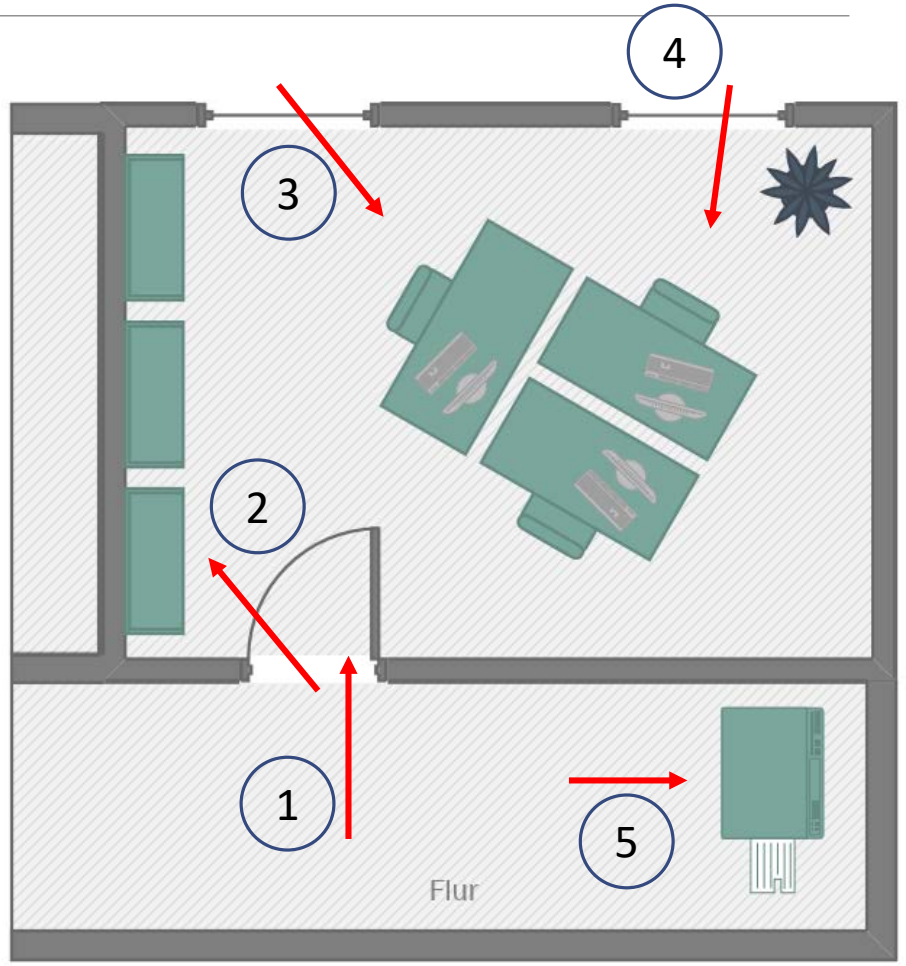
Zugang zu Daten

Welche möglichen Gefahren ergeben sich hier?



Zugang zu Daten

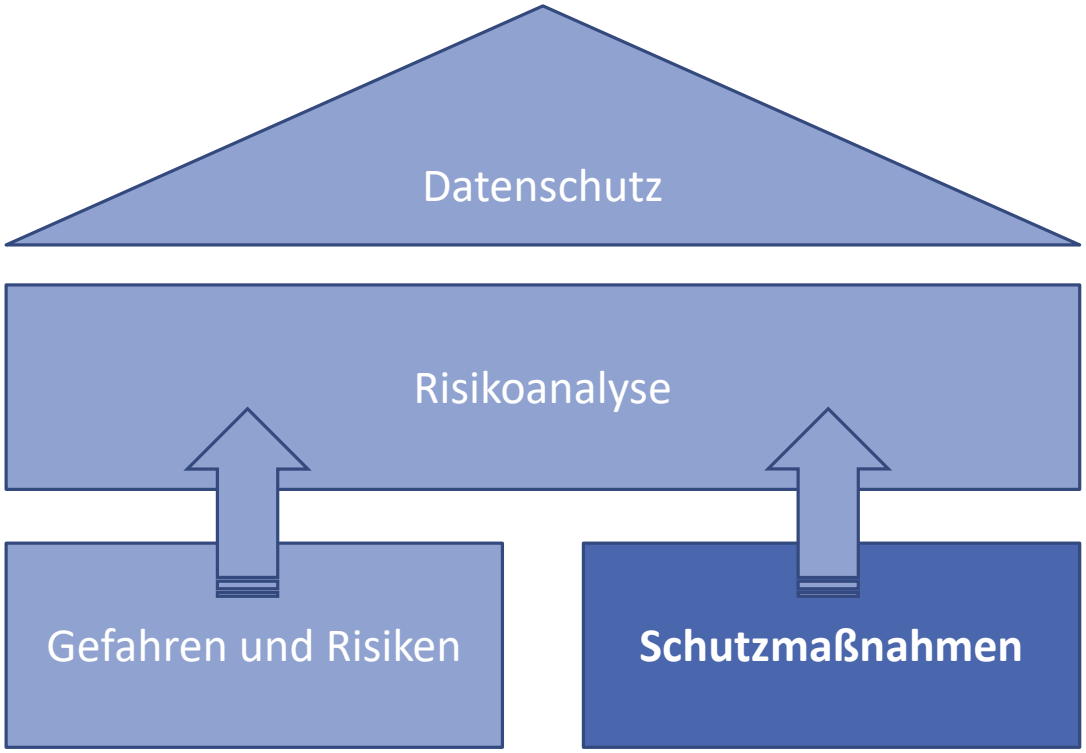
(1) Frage nach Zutrittsberechtigung („Wer hat alles einen Schlüssel?“).
(2) Leichter Zugriff auf Akten im Regal bei offener Tür.
(3) Einsicht auf Bildschirminhalte durch das Fenster.
(4) Möglicherweise Zutritt durch das Fenster und somit Zugriff auf die Arbeitsplätze.
(5) Zutritt und Zugriff auf den Kopierer.



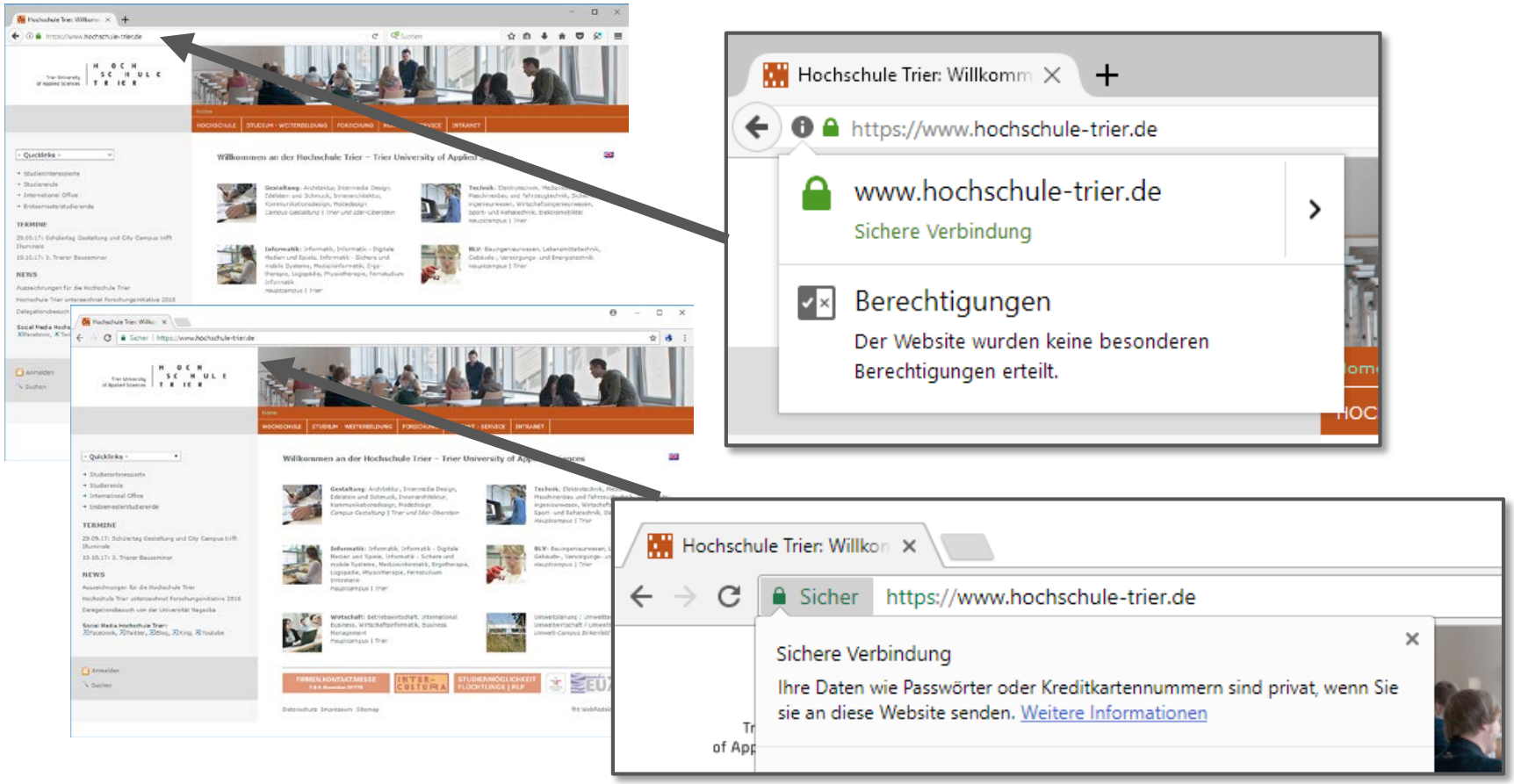
Weitere Gefahren

- Shoulder Surfing: Beobachtung „über die Schulter“ bei Passworteingabe
  → Auf verdeckte Eingabe achten.
- Dumpster Diving: Der Abfall wird nach personenbezogenen Daten oder sonstigen sensiblen Informationen durchsucht. Dies umfasst sowohl Papierdokumente als auch Hardware (Festplatten).
  → Auf ordnungsgemäße Entsorgung achten.
- Skimming: Auslesen von PIN und Magnetstreifen durch angebrachte Vorsatzgeräte an Geldautomaten (und Tankstellen).
- Weitere Physische Risiken: Diebstahl, Brand, höhere Gewalt, etc.

Schutzmaßnahmen



Verschlüsselte Webseiten

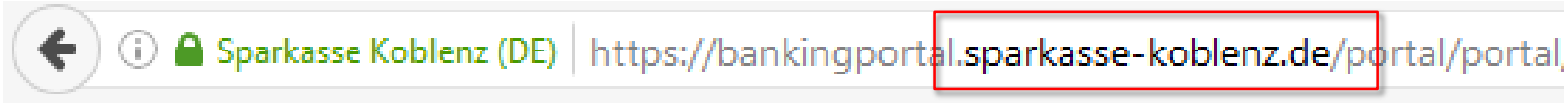


Verschlüsselte Webseiten

1. Ohne Schutz: Keine Sicherung:

2. Schutz der Adresse: Überprüfung, dass ich mich tatsächlich auf der Webseite (Adresse) befinde, die im Zertifikat angegeben wird:

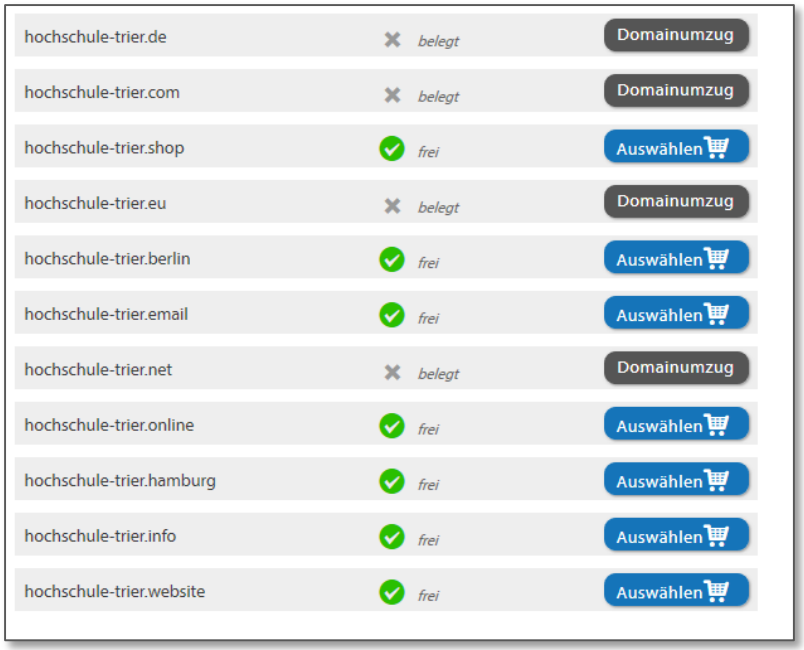
3. Schutz der Organisation: Überprüfung, dass ich mich tatsächlich auf der Webseite befinde und diese der genannten Organisation gehört:



Verschlüsselte Webseiten

Kein Schutz:

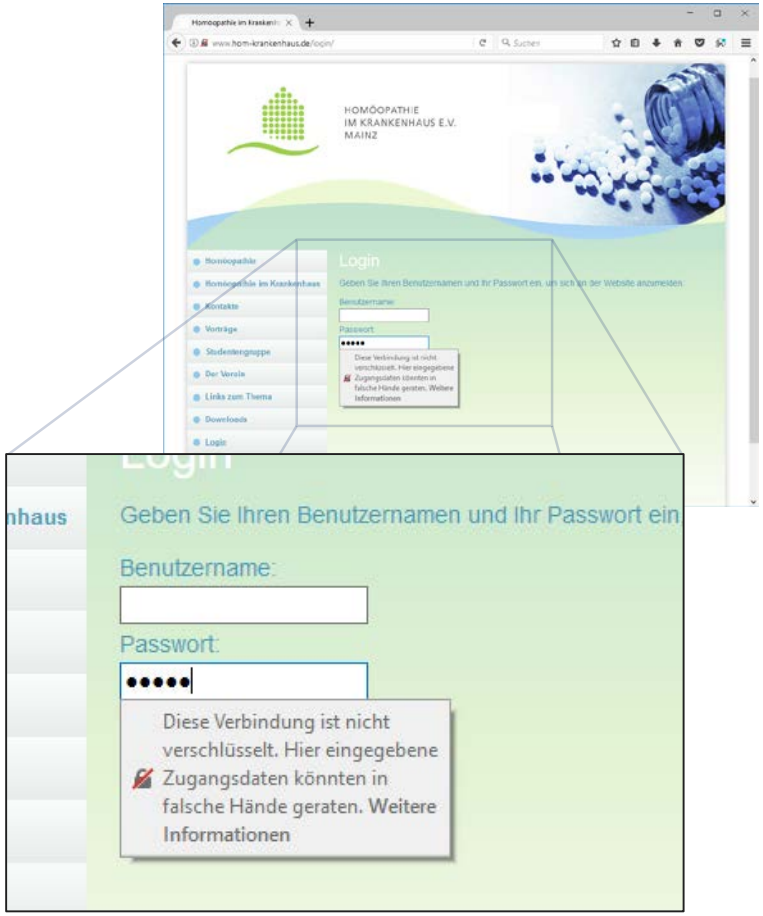
- Bei einem kompromittierten System (z.B. an öffentlichen Rechnern oder bei Infektion mit Schadsoftware).
- Bei Tippfehler oder Varianten der Adresse:
  - hochschule-bier.de
  - hochschuletrier.de
  - hochschule-trier.info
- Bei Unteradressen (Subdomains):
  - hochschule-trier.imweb.de
  - hochschule-trier.de.vu
- bzgl. Inhalt / Richtigkeit / Sicherheit der Webseite selbst.



Quelle: Strato.de am 10.10.2017

Verschlüsselte Webseiten

- Benachrichtigung bei unverschlüsselter Passwortübertragung seit Firefox 52.
- Ggf. Prüfung ob die Adresse auch über https://... erreichbar ist: http://gmx.de -> https://gmx.de
- Insbesondere kritisch, wenn die Warnung früher nicht zu sehen war
- „Erziehungsmaßnahme“ für den Webseitenbetreiber



Sichere Passwörter

- Passwort mind. 8 Zeichen, besser 12, nicht aus einem Wörterbuch.
- Sonderzeichen erhöhen zwar die Sicherheit leicht, erschweren jedoch den Umgang.
- Änderungen weniger regelmäßig, sondern mehr nach Bedarf.
- Passwörter für verschiedene Dienst bzw. verschiedene Sicherheitsstufen.
- Strategien zur Generierung sicherer Passwörter…

Sichere Passwörter (Strategien)

Strategien zur Generierung guter Passwörter:

- aus einem Satz:

Ich **h**abe **g**elernt **w**ie **m**an **s**ichere **P**asswörter **e**rstellt **u**nd **m**erkt

→ „IhgwmsPeum“

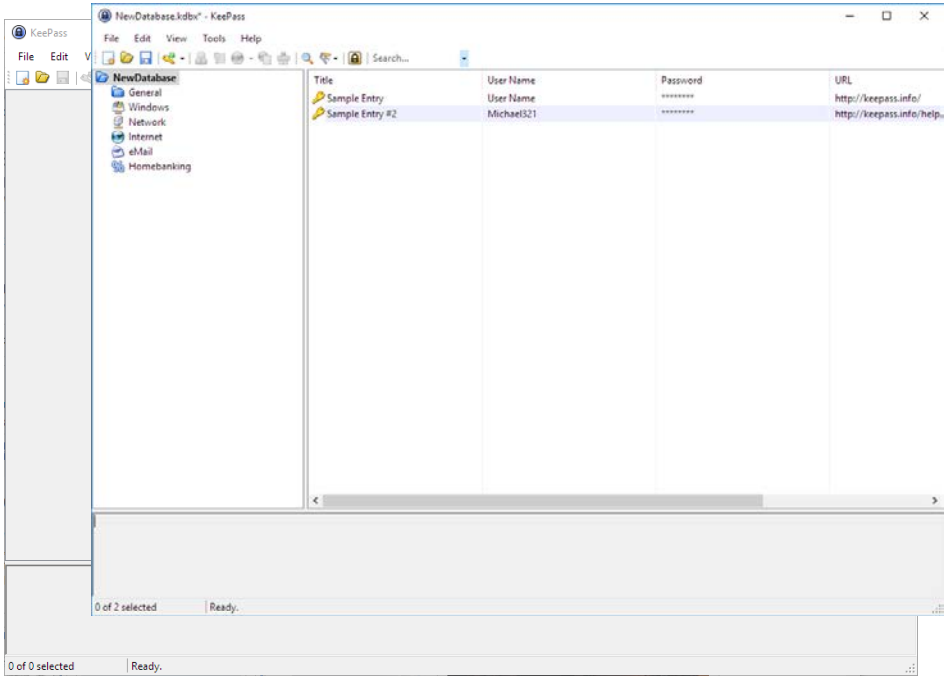
- aus mehreren (mind. fünf) Wörtern:

→ „Übermorgen Hund Waffel Auspuff Klavier“

(jedoch problematisch wenn Passwörter abgeschnitten werden)

Sichere Passwörter (Tresore)

- Schutz von Passwörtern durch ein (starkes) Masterpasswort
- Zwei Arten:
  - Lokale Speicherung der Passwörter (z.B. Keepass)
  - Speicherung der Passwörter in „der Cloud“ (z.B. Lastpass).
    Aber: Vertraulichkeit? Verfügbarkeit?



Keepass Passworttresor v2.36

Sichere Datenlöschung

- „Einfaches“ Löschen von Dateien oder Formatieren von Festplatten bewirkt keine endgültige Löschung, Wiederherstellung ist weiterhin möglich.
- Datenträger (USB-Sticks, Festplatten) sollten daher sicher gelöscht oder physikalisch zerstört werden. Ggf. Rückfrage mit dem Rechenzentrum halten.

Weitere Infos: BSI Empfehlung zur Datenlöschung

Gesunder Menschenverstand

„Vertrauen Sie Meldungen, Nachrichten und Aufforderungen nicht blind. Klicken Sie nicht auf jedes Angebot, auch wenn es noch so verlockend klingt. Denn auch im Internet gibt es nichts umsonst. Viele Anbieter, die mit Preisen und Belohnungen locken, wollen nur an Ihre Daten. Manche versuchen eventuell später, Ihre Daten weiterzuverkaufen oder durch spezielle Schadsoftware an weitere Daten von Ihnen zu kommen. […]“

Quelle: BSI für Bürger (BSIFB) am 10.10.2017

Aktuelle Themen

- **Disqus-Plattform bereits 2012 gehackt** (Oktober 2017)
  - Mitteilung erst Oktober 2017
  - Nutzername + Passwort(hash) von 17 Mio Nutzern geleakt
  - „Kritisch“ wenn Passwörter mehrfach genutzt werden

- **Schadcode in CCleaner 5.33.6162 Software** (September 2017)
  - CCleaner ist ein Bereinigungstool für Windows
  - Malware CCleaner-Software entdeckt
  - geschätzt 2,27 Mio Betroffene
  - Update auf neue Version empfohlen

Aktuelle Themen

- **Lücke in Nvidia GPU-Treiber** (September 2017)
  - Ermöglicht die Erhöhung von Berechtigungen (Administratorrechte)
  - Aktualisierung steht zum Download bereit

- **Beraterunternehmen Deloitte ziel eine Hackerangriffs** (September 2017)
  - Angreifer erreichten Administratorrechte auf schlecht abgesicherten E-Mail Server
  - Zugriff auf alle (unverschlüsselt) gesendet und empfangenen E-Mails
  - ca. 5 Mio E-Mails
  - Deloitte selbst Beratungsunternehmen für „Cybersicherheit“

Aktuelle Themen

- **Malware zum „Mining“ von Kryptowährungen**
  - IBM spricht von Versechsfachung von Mining-Malware
  - Auffällig durch besonders intensive Systemnutzung
  - Quelle: trojaner-info.de

- **Trojaner „Retefe“ nutzt nun auch SMB-Schwachstelle EternalBlue**
  - Alt: Infektion des Rechners über Makro in einem Word-Dokument, Installation eines eigenen CA-Zertifikats, Ziel: PINs/TANs beim Onlinebanking
  - Neu: Malware sucht im Netzwerk nach Infektionsmöglichkeiten über SMB-Schwachstelle (Wurm-Funktionalität)
  - Quelle: botfrei.de

Weitere Informationen

Allgemeine Informationen

- BSI für Bürger: https://www.bsi-fuer-buerger.de
- Aufsicht für den Datenschutz RLP https://www.datenschutz.rlp.de/de/themenfelder-themen/selbstdatenschutz/
- Webseite des Rechenzentrums der Hochschule Trier

News

- Heise (Security) News: https://www.heise.de/security/news/
- Sicherheitshinweise beim Bürger-CERT: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Buerger-CERT/Buerger-CERT_node.html