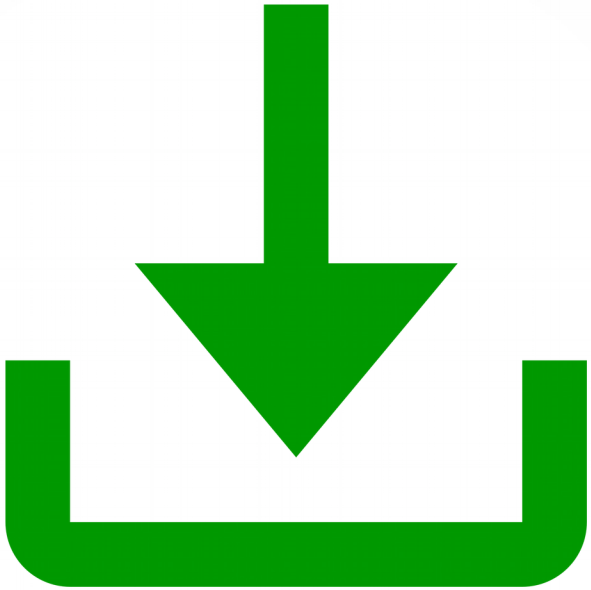
BÜNDNIS 90
DIE GRÜNEN
REHLINGEN-SIERSBURG

IT-Sicherheit
Grundwissen für den Alltag

13.05.2019 | Benjamin Mey

Präsentation online verfügbar

https://gruene-resi.de/it-sicherheit



- Ab Montag zum freien Download verfügbar

Themen

- Wie, hier geht es nicht um Datenschutz?
- Ich habe nichts zu verbergen!
- Auf mein Passwort kommst du nie!
- Ist E-Mail nicht eher so 90er?
- Wie viele Megapixel hat dein Handy so?
- Meine Bankfiliale ist online!
- Have I been pwned?

Wie, hier geht es nicht um Datenschutz?

Der Beginn der Weisheit ist die Definition der Begriffe.

Sokrates

Was soll das sein?

DSGVO

Cyber Security

Social Engineering

Informationssicherheit

IT-Sicherheit

Datenschutz

Worum geht es heute?

Datenschutz

- Gesetzliche Vorgaben für alle Datenverarbeiter (Unternehmen, Vereine, Organisationen, ...)
- Gilt nur für **nicht privat** verarbeitete **personenbezogene** Daten.
- EU-Verordnung (allgemeingültiges Gesetz für alle EU-Mitgliedsstaaten) DSGVO
- Aufgabe der Datenverarbeiter, **nicht der Nutzer/Kunden/Mitglieder**.

Worum geht es heute?

Persönliche IT-Sicherheit

- Eigene Maßnahmen um die Nutzung von Geräten und Online-Diensten so sicher wie möglich zu machen
- Unwissenheit der Nutzer und unbedarfte Nutzung ist die am leichtesten auszunutzende Schwachstelle von Geräten und Online-Diensten
- Eigene Maßnahmen zum Schutz der eigenen Daten
- Datenschutz von Verarbeiter hilft wenig, bei fahrlässigen Verhalten von Dateneigentümern

Worum geht es heute?

Social Engineering

Hallo Herr Müller hier ist ihr Microsoft Update Service. Wir haben Probleme beim Aufspielen neuer Sicherheitsupdates auf Ihren Rechner. Wir bräuchten zur **schnellen** Reparatur ihr Passwort!

Ähm. Ok...mein Passwort ist XyZqWe90 .

Worum geht es heute?

Social Engineering: 2,3 Milliarden US-Dollar Schaden durch CEO-Betrugsmasche

08.04.2016 16:28 Uhr – Axel Kannenberg vorlesen

(Bild: dpa, Ralf Hirschberger)

Betrüger geben sich in E-Mails als Chef oder Handelspartner aus und veranlassen arglose Mitarbeiter zu hohen Überweisungen vom Geschäftskonto. Diese Masche greift laut FBI immer mehr um sich und sorgt für Milliardenschäden.

Worum geht es heute?

Social Engineering

- *„zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.“*
- Mittlerweile die am weitesten verbreitete Form der Angriffe von Cyber Kriminellen
- „Social Hacking“ oder „Menschen hacken“

Ich habe nichts zu verbergen!

Habe Mut, dich deines eigenen Verstandes zu bedienen!

Immanuel Kant

Wann sind meine Daten sicher?

- Einfache Antwort: Nie!
- Längere Antwort: In der Informationstechnologie gibt es den Zustand „sicher“ nicht. Es gibt nur „ausreichend sicher“.
- IT-Sicherheit heißt immer Risiko und Nutzen abzuwägen.
- Man kann durch eigene Maßnahmen ein Risiko erheblich erhöhen und erheblich reduzieren, aber nie gänzlich vermeiden.

Sind alle meine Daten gleich?

- Nicht alle Daten sind gleich sensibel!
- Grundsätzliche Einteilung in:

  - ***Geht Niemanden etwas an***
  - **Sollen nur ausgewählte Personen sehen**
  - **Darf jeder wissen**

Daten unterscheiden

Schadenspotential

- Unterscheidung nach Schadenspotential bei Verlust / Manipulation
- **Schadensszenarien:** öffentlicher Gesichtsverlust, wirtschaftlicher Schaden, Identidätsdiebstahl, Betrugspotential, Belästigung, Erpressung...

  - ***Großer bis existenzieller Schaden***
  - ***Evtl. möglicher Schaden***
  - ***Kein bis unerheblicher Schaden***

Daten unterscheiden

Beispiele

- **Rote Daten:** Passwörter, Zugangsdaten...
- **Gelbe Daten:** E-Mail Adresse, Telefonnummer, Medizinische Daten, Kontonummer, mir anvertraute Daten, Anschrift, Bewegungsdaten, (Kauf-)Gewohnheiten, Familienfotos...
- **Grüne Daten:** Wohnort, Haarfarbe, Pseudonym, eigene Fotos ohne Personen, Kopien erworbener elektronischer Medien (Bücher, Musik, Videos),...

Unterschiedlich behandeln

- Wahrscheinlichkeit für Verlust vor Augen halten
- Vertraulichkeit von Verarbeitern bewerten

  - ***Immer nur verschlüsselt Online-Diensten anvertrauen. Nur auf sicheren eigenen Geräten (verschlüsselt) speichern.***
  - **Nur mit vertrauenswürdigen Online-Diensten teilen. Wenn möglich verschlüsseln. Nur auf eigenen Geräten speichern.**
  - **Ohne Einschränkung, je nach praktischen Nutzen speichern und teilen.**

Unterschiedlich behandeln

Vertrauenswürdigkeit Online-Dienst?

- Geschäftsmodell betrachten!
  - ***Kostet eine Dienstleistung im Internet nichts, ist man nicht Kunde, sondern Produkt.***
- Datenschutzerklärung lesen (zumindest überfliegen, grundsätzlich verständlich?).
- Impressum suchen und lesen (Seriös?)
- Nach Person/Unternehmen aus Impressum im Internet suchen
- Sind Datenschutzvorfälle schon bekannt geworden? Umgang in der Öffentlichkeit damit?
- Unternehmensstandort in Europa?

Vertrauenswürdigkeit

Beispiel Google

- **Geschäftsmodell:** Vermittlung von Werbung an Zielgruppen mit passenden Interessen/Motivationen. Private Nutzer von Google Dienste werden nach Interessen bewertet und profilisiert. Dafür Dienste ohne Gebühr nutzbar.
- **Datenschutzerklärung:** Komplex und umfangreich, aber grundsätzlich DSGVO konform, transparent und verständlich. Google verheimlicht weder Geschäftsmodell noch Absichten.
- **Unternehmensstandort:** USA. Verpflichtungen gegenüber US-Regierung/Geheimdiensten.
- **Bewertung:** Umsatz und Gewinn von Google sind davon abhängig, dass Niemand außer Google über die gesammelten Daten verfügt. Anvertraute Daten zumindest vor Dritten relativ sicher. Grüne Daten auf jeden Fall, gelbe unter Umständen besser vor Dritten geschützt als zu Hause.

Daten unterscheiden

Verfügbarkeit der Daten?

- Wie kritisch wäre ein Datenverlust?
- Wie oft will ich auf die Daten zugreifen?
- Wo möchte ich auf die Daten zugreifen?
- Sollen andere bequem auf die Daten zugreifen können?

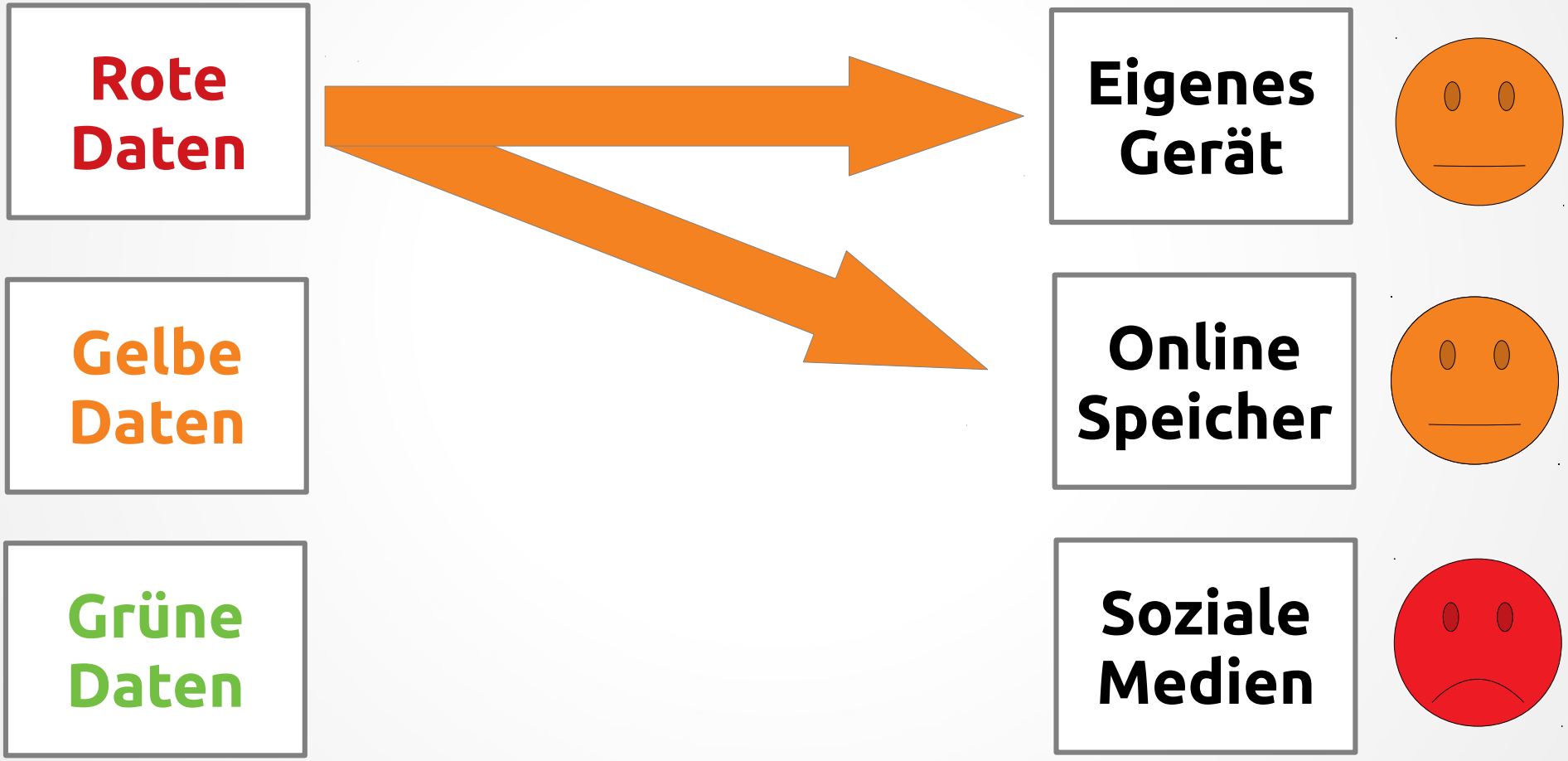
Daten unterscheiden

Online-Dienste?

- **Online Speicher**
  - Cloud Speicher („online Festplatte“)
  - E-Mail Anbieter
  - Online Kontakte / - Kalender
  - Fotogallerie
- **Soziale Medien**
  - Facebook, Instagram, WhatsApp...

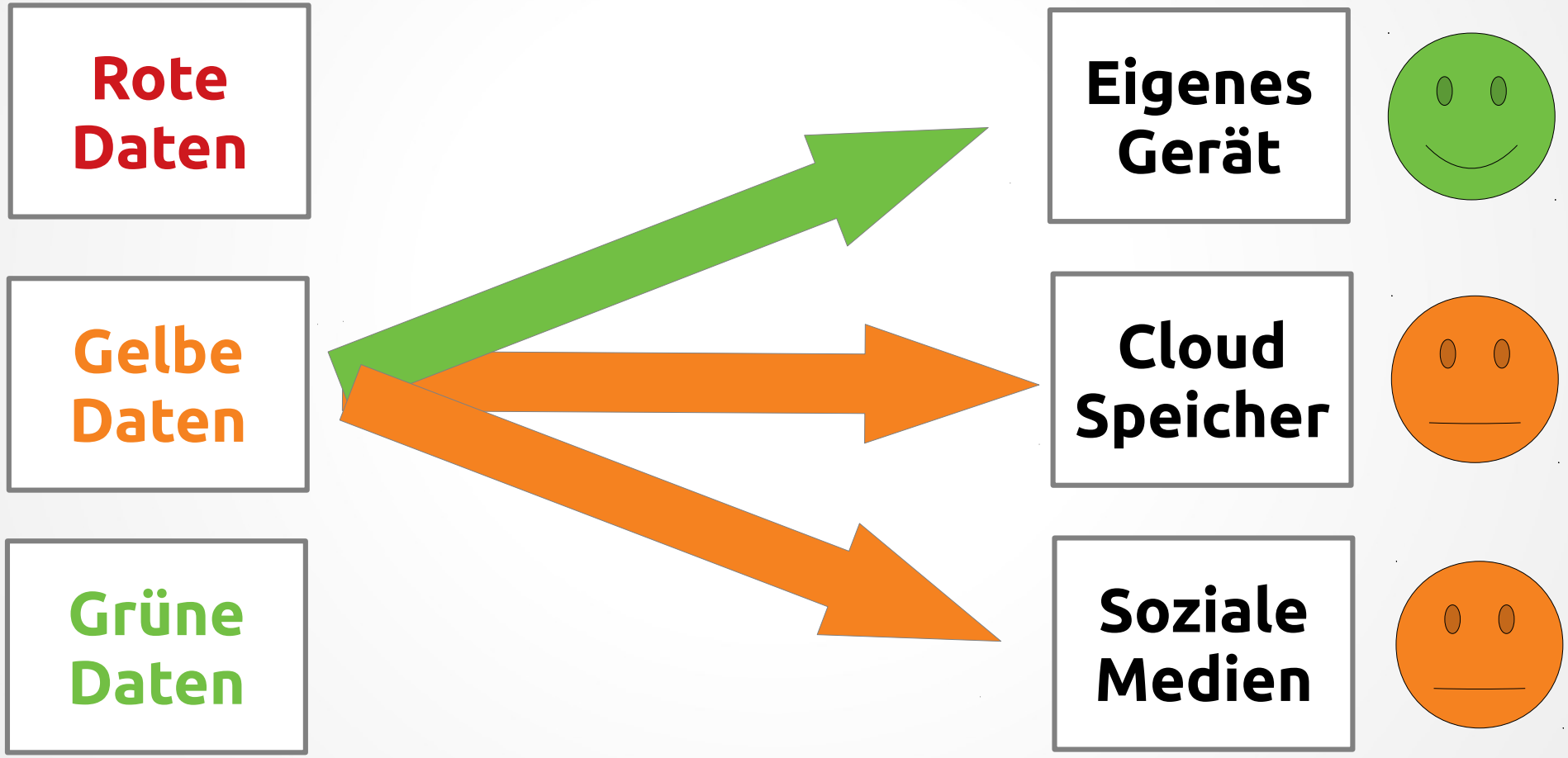
Daten unterscheiden

Wo speichern?



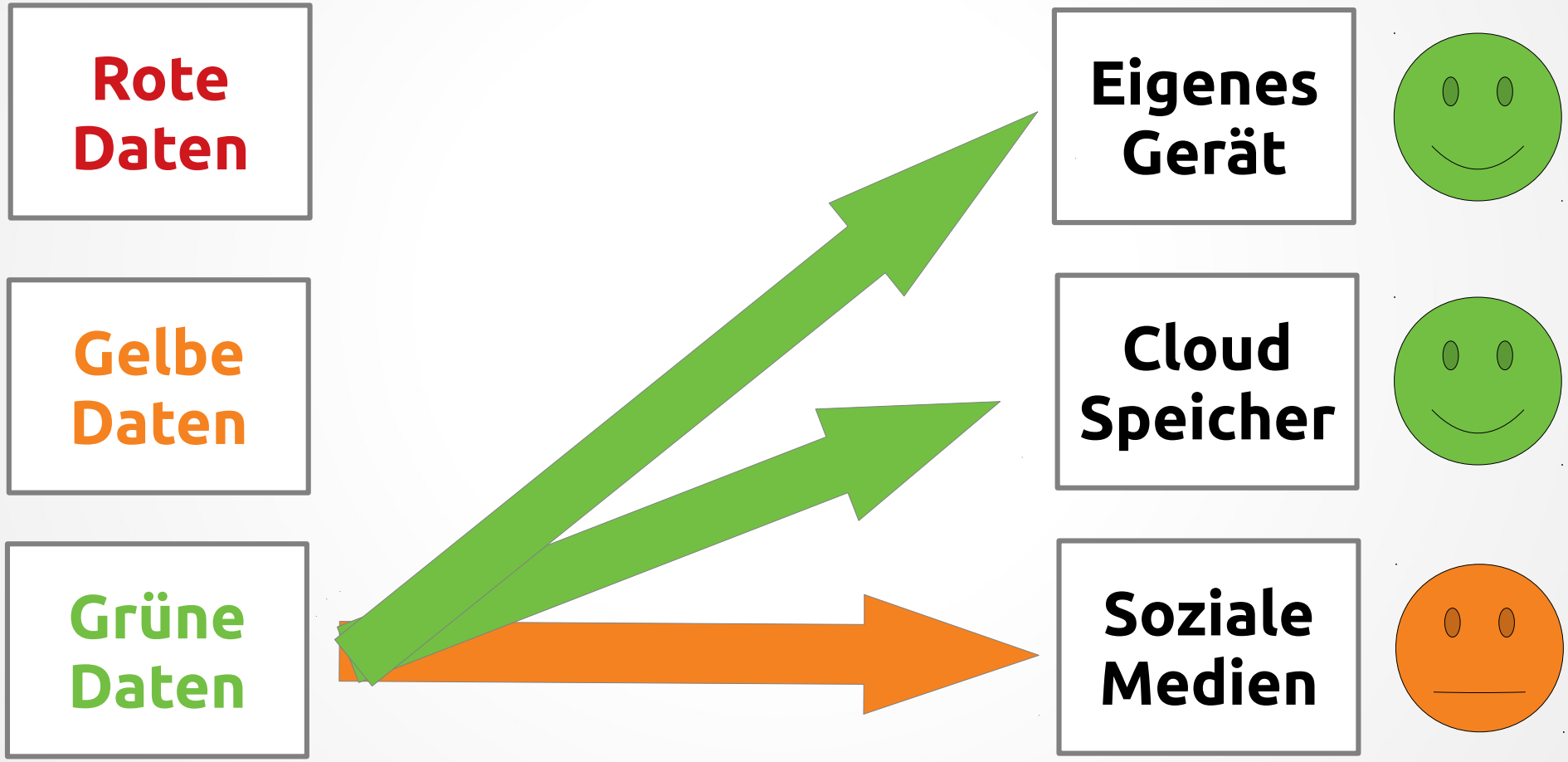
Daten unterscheiden

Wo speichern / benutzen?



Daten unterscheiden

Wo speichern / benutzen?



Auf mein Passwort kommst du nie!

Was einer weiß, weiß keiner. Was zwei wissen, wissen alle.

Aus Schweden

Millionen Zugangsdatensätze für Mail-Provider im Netz

05.05.2016 10:46 Uhr – Volker Briegleb vorlesen

(Bild: dpa, Julian Stratenschulte)

Ein russischer Hacker bietet in einschlägigen Foren offenbar eine riesige Sammlung von Zugangsdatensätzen an. Darunter soll auch einiges an Frischware sein, sagt ein Sicherheitsexperte.

Ein Sicherheitsexperte hat laut einem Agenturbericht die Daten von 272 Millionen E-Mail-Accounts von einem russischen Hacker erhalten. Ein Großteil davon seien

Identitätsklau: Hasso-Plattner-Institut zieht Bilanz

30.12.2015 16:38 Uhr – André von Raison vorlesen

Im Lauf des ausgehenden Jahres haben Sicherheitsforscher 15 Vorfälle mit von Cyberkriminellen veröffentlichten Identitäten analysiert. 35 Millionen Datensätze später bleibt die ernüchternde Erkenntnis, dass zu simple Passwörter nicht tot zu kriegen sind.

Rang	Passwort	Häufigkeit in Promille
1	123456	10,37
2	123456789	3,49
3	12345678	1,94
4	password	1,85
5	qwerty	0,95
6	adobe123	0,91
7	1234567	0,69
8	111111	0,67
9	12345	0,61
10	1234567890	0,51

Geheimnis eines guten Passworts

Was man so kennt?

- Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen
- 8 Zeichen lang
- Jeden Monat ändern
- Keine bekannten Wörter verwenden
- Nicht notieren, nicht speichern, auswendig lernen

Geheimnis eines guten Passworts

Welches Passwort ist besser?

- **A:**
  $pGf2t!Q

- **B:**
  PetersEinhornwohntingruenenBa
  umwollhuetten

Geheimnis eines guten Passworts

Richtige Antwort: B

- **A:** Theoretische Zeit zum berechnen mit einem normalen Computer:
  - **max. 93 Tage**
- **B:** Theoretische Zeit zum berechnen mit einem normalen Computer:
  - **Mehrere Mio. Jahre**

Vorsicht Hacking-Theorie

Was ist Brute Force?

- Passwörter werden aus Datenbanken gestohlen
- Passwörter sind Einweg-Verschlüsselt (normalerweise)
- Computerprogramm berechnet zufällige Kombinationen von Passwörtern und verschlüsselt sie nach dem Schema in der Datenbank
- Wird Übereinstimmung gefunden: Passwort entdeckt!

Vorsicht Hacking-Theorie

Einwegverschlüsselung?

- Mathematische Berechnung eines „Hash-Werts“ aus einem Passwort.
  - Passwort: „Geheim“
  - Hash-Wert (SHA-256): „d768ccc827c5d0aab5a460185dfbce2fb4f144f60edaa3cb66af9c086b03d87e“
- **Keine** „Rückberechnung“ von Hash-Wert zu Passwort möglich. Daher muss das Passwort „erraten“ (= zufällig berechnet) werden.

Geheimnis eines guten Passworts

Passwortlänge	Maximale Zeit für erfolgreichen Brute Force-Angriff		
Zeichen	26	52	96
6	0 Sekunden	22 Sekunden	15 Minuten
7	9 Sekunden	19 Minuten	23 Stunden
8	4 Minuten	17 Stunden	93 Tage
9	2 Stunden	36 Tage	25 Jahre
10	44 Stunden	5 Jahre	2.342 Jahre
11	47 Tage	265 Jahre	224.872 Jahre
12	3 Jahre	13.772 Jahre	21.587.666 Jahre
13	87 Jahre	716.134 Jahre	2.072.415.888 Jahre
14	2.272 Jahre	37.238.973 Jahre	198.951.925.262 Jahre
15	59.095 Jahre	1.936.426.593 Jahre	19.099.384.825.135 Jahre

Zusammengefasst

Auf die Länge kommt es an!

- Besser so lang wie möglich, als so komplex wie möglich
- Wörter sind nur dann schlecht, wenn man sie einzeln benutzt.
- Wörter können wir uns besser merken als kryptische Zeichenfolgen
- Besser ein sehr langes Passwort lange benutzen als ständig ein neues.
- Besser merken als aufschreiben oder „irgendwo“ speichern

Aber aber...

Wenn es doch kurz sein muss

- Zufälligen Satz im Kopf ausdenken mit Zahlen und Sonderzeichen
  - „*Sie hieß Bella, ich war 12, sie ein Hund.*“
- Die Anfangsbuchstaben, Zahlen und Satzzeichen als Passwort nutzen:
  - „ShB,iw12,seH.“

So viele Passwörter

Für jedes Konto ein eigenes

- Entweder an den Anfang des langen Passwortsatzes den Dienst schreiben
  - „**FaceBook**PetersEinhornwohntingruenenBaumwollhuetten“
- Oder an den Anfang des kurzen Passworts
  - „**FB**ShB,iw12,seH.“
- **So werden aus zwei guten Passwörtern unendlich viele sichere Passwörter.**
- Zwei Passwörter kann man sich merken

Ist E-Mail nicht eher so 90er?

In einer neuen Sache steckt viel Altes.

Hubert Joost

Warum ist E-Mail so wichtig?

Das E-Mail Postfach...

- Ist **das wichtigste Benutzerkonto** im Internet
- Ist die unsicherste Art im Internet zu kommunizieren
- Ist die älteste Kommunikationsform im Internet
- Ist der am häufigsten genutzte Weg von Cyber Kriminellen

Warum ist E-Mail so wichtig?

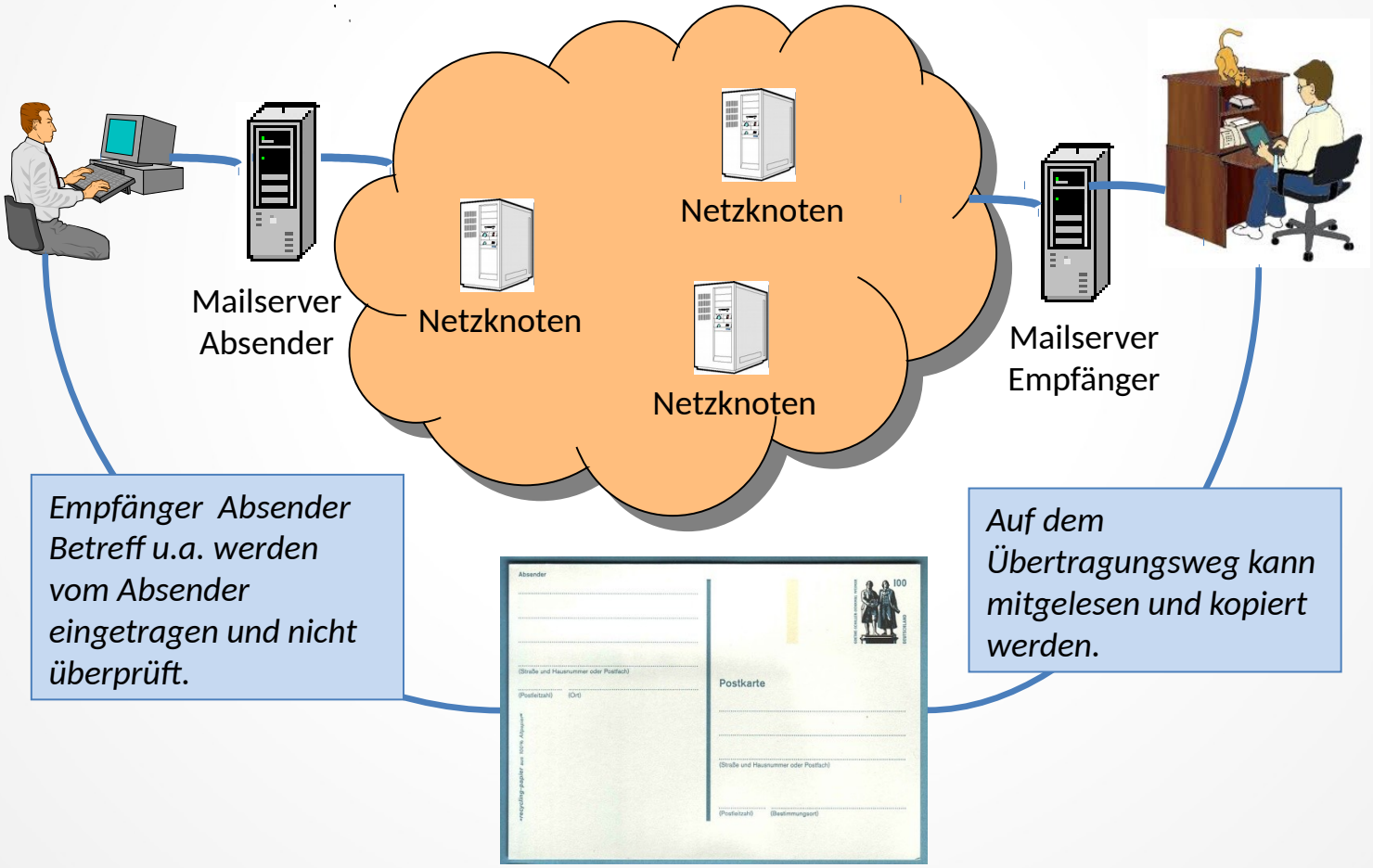
...das wichtigste Konto

- „Passwort vergessen“
- Benutzername = E-Mail Adresse
- Meist genutzter Dienst im Internet

Warum ist E-Mail so wichtig?

...die unsicherste Art...

Überblick E-Mail-Infrastruktur



Warum ist E-Mail so wichtig?

...die älteste Kommunikation...

- Ray Tomlinson hat im Jahr 1971 den ersten elektronischen Brief verschickt und gilt seitdem als Erfinder der E-Mail.
- Protokoll bis heute grundsätzlich unverändert, nur um <u>optionale</u> Sicherheit erweitert.

Warum ist E-Mail so wichtig?

...Werkzeug von Kriminellen...

- Kostenlos
- Sehr einfach zu fälschen
- Unverschlüsselt und unsigniert möglich
- E-Mail Adressen massenhaft bekannt und zugänglich
- Fehlendes Bewusstsein der meisten Nutzer

Warum ist E-Mail so wichtig?

Worauf achten?

- E-Mail Provider sorgfältig auswählen
- Nur verschlüsselter Abruf und Versand über E-Mail Programme und Apps (SSL/TLS)
- Niemals rote Daten per Mail verschicken
- Vorsicht bei gelben Daten
- E-Mail immer als Postkarte des Internets betrachten

Warum ist E-Mail so wichtig?

Worauf achten?

- Traue keinem Link, den du nicht selbst getippt hast!
- Jede E-Mail ist eine potentielle Phishing Mail, bis man sich vom Gegenteil überzeugt hat!
- Erst schauen, dann klicken!

Warum ist E-Mail so wichtig?

Traue keiner URL die du nicht selbst getippt hast...
Benjamin Mey An: benjamin.mey

Schau mal hier

Toller Artikel, schau mal :https://heise.de/developer/meldung/Nachholbedarf-beimSecurity-Wissen.html

Mit freundlichen Grüßen

SPARKASSE MERZIG-WADERN
Benjamin Mey
Informationssicherheitsbeauftragter

http://www.schnapp-den-virus.ru/

Traue keiner URL die du nicht selbst getippt hast...
Benjamin Mey An: benjamin.mey

Schau mal hier

Toller Artikel, schau mal :https://heise.de/developer/meldung/Nachholbedarf-beimSecurity-Wissen.html

Mit freundlichen Grüßen

SPARKASSE MERZIG-WADERN
Benjamin Mey
Informationssicherheitsbeauftragter

http://und-hier-gibts-gleich.de/n/naechsten/virus/fuer/dich.html

Phishing E-Mail?

Typisch für Phishing-Mails:

- Bla Bla Bla… klicke hier … bla bla bla
- Gefahr, schnell hier klicken sonst …
- Bitte Daten eingeben, und zwar hier…
- Sie haben gewonnen, klicken Sie hier…
- Wir berechnen, hier klicken für die Rechnung…
- **Wer solche Mails schreibt, legt keinen Wert auf Seriosität!**
- **Solche Mails grundsätzlich ignorieren!**

Phishing E-Mail?

Typisch für Phishing-Mails:

- Absender Name von bekannten Kontakt, aber unbekannte E-Mail Adresse
  - **Gefälschte Mail**
- Absender Name und Adresse von bekannten Kontakt
  - **Absender evtl. mit Virus infiziert**

Achtung wichtiges Grundwissen!

Aufbau einer Internet URL:

https://www.google.de/

Übertragung

http:// = unverschlüsselt
https:// = verschlüsselt

Subdomain(s)

Alles vor dem Punkt der Domain sind Subdomain(s)

Domain

Der Text vor dem letzten Punkt ist die eigentliche Domain

TLD

Der Text zwischen dem ersten / und dem Punkt davor ist die Top Level Domain (z.B. Land)

Seriös oder Unseriös?

Beispiel-URLs:

https://www.google.de.suche.ru/index.php

http://www.zdf.de.mediathek.aq/index.html

http://www.sparkasse.de.tokenID-%TW3erg.com/login.php

Seriös oder Unseriös?

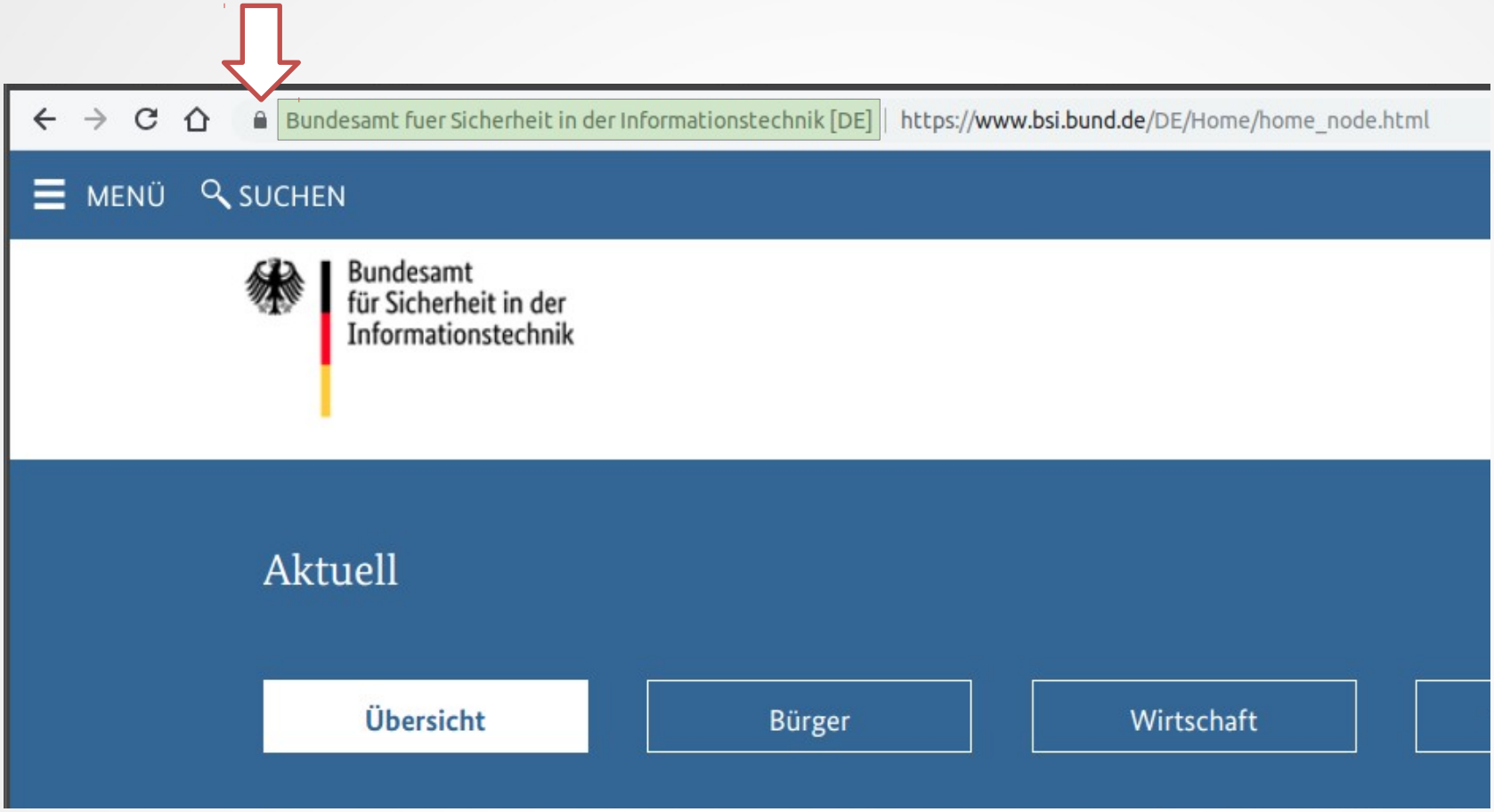
https://www.google.com/ru/index.php

https://konto.deka.de.vu/postfach.php

http://www.faz.de/vu.ru/download.asp

https://www.amazon.co.uk/s?k=Lovecraft

Seriös oder Unseriös?



Seriös oder Unseriös?

Gefährliche Datei-Anhänge

Dateianhänge (Windows)

- .exe .com .cmd .bat – NIEMALS öffnen
  - Kein Dokument, ausführbares Programm
  - Niemals seriös, besser löschen / ignorieren
- .doc .docx .xlsx .xls … - Office Dateien.
  - Möglicherweise gefährlich
  - Ungeeignet für reinen digitalen Dokumentenaustausch
  - Bearbeitungsdokumente und keine Lesedokumente
  - Können Schadcode enthalten
  - Ggf. Absender Rückfragen, wenn unerwartet empfangen

Gefährliche Datei-Anhänge

Dateianhänge (Windows)

- .pdf – „Digitale Ausdrucke“
  - Empfohlenes Dokumenten Austausch-Format
  - Deutlich Geringeres Risiko für Schadcode
  - Immer PDF-Dokumente bevorzugen, auch beim Versenden

Wie viele Megapixel hat dein Handy so?

Ach ja, die Statussymbole werden auch immer kleiner.

Siegfried Wache

Worauf achten beim Gerätekauf

Welche Features braucht man?

- Kein Gerät und kein System ist dauerhaft sicher!
- Sicher sind Geräte immer nur für kurz
  - kurz nach dem Update!
- Sicherheitsupdates / App-Updates / Version-Updates…

Worauf achten beim Gerätekauf

Fragen vor dem Kauf?

- Ist der Softwarestand aktuell?
- Wie lange garantiert der Hersteller Updates?
- Wie pünktlich kommen die Updates?

Worauf achten beim Gerätekauf

Android (Google) oder iOS (Apple)?

- Apple ist vorbildlich was Update-Versorgung alter Geräte angeht!
- Android Updates sind normalerweise vom Hardwarehersteller abhängig, nicht von Google
- „Android One“ Geräte oder Geräte direkt von Google (Pixel-Reihe) sind ebenfalls vorbildlich was Update-Versorgung angeht.

Worauf achten beim Gerätekauf

Was ist mit Windows?

- Windows 10 ist aktuell und erhält regelmäßig Updates.
- Windows Phones sind veraltet und erhalten keine Updates mehr
- Windows 10 Tablets erhalten ebenfalls regelmäßig Updates.

Worauf achten beim Gerätekauf

Virenschutz?

- Apple iOS Geräte (iPhones & iPads) mit aktuellen Versionen benötigen keine Virenschutzsoftware
- Android Geräte mit aktuellen Sicherheitsupdates benötigen keine Virenschutzsoftware
- Windows 10 hat einen guten Virenschutz kostenlos inkl. Für Privatnutzer ist dieser in der Regel ausreichend zum Schutz vor Viren.

Worauf achten beim Gerätekauf

Virenschutz?

- Virenschutz überbrückt die Zeit zwischen entdeckter Sicherheitslücke in Betriebssystem und Update.
- Im Wesentlichen nur für Windows wichtig.
- Apple App-Store und Google Play-Store haben einen Virenschutz integriert
- Apps nur aus den offiziellen App-Stores kaufen und herunterladen. Keine Drittanbieter verwenden.
- Virenschutzsoftware für Android ersetzt keine Sicherheits-Updates. In der Regel nicht sinnvoll.

Worauf achten beim Gerätekauf

Keine Updates mehr?

- Geräte für die keine Updates mehr bereitgestellt werden, sollten ausgetauscht werden.
- Android One oder Google Pixel Geräte ca. alle 3-4 Jahre. Android-Geräte von anderen Herstellern häufig schon nach 1 Jahr.
- iOS Geräte häufig länger, unterschiedliche Zeit.

Meine Bankfiliale ist online

Eine Bank ist ein Institut bei dem man Geld leihen kann, gegen den Nachweis, dass man es nicht braucht.

Unbekannt

Ist Onlinebanking sicher?

Wie riskant ist Onlinebanking?

- **Einfache Antwort:** Kommt darauf an!
- **Längere Antwort:** Je nach TAN-Verfahren, benutztem Gerät und eigenem Verhalten kann Onlinebanking sehr sicher sein, aber auch sehr unsicher.

Ist Onlinebanking sicher?

Wie gehts richtig?

- Alle bereits erwähnten Methoden zu Verbesserung der persönlichen IT-Sicherheit gelten im erhöhten Maße für das Onlinebanking.
- Für das Onlinebanking kommen noch weitere sinnvolle Regeln dazu.

Ist Onlinebanking sicher?

Sichere TAN-Verfahren?

- Chip-TAN (QR) gilt als das umständlichste und gleichzeitig sicherste Verfahren nach aktuellem Stand.
- Direkt gefolgt von Push-TAN über eine dedizierte Push-TAN Smartphone App der Bank.

Ist Onlinebanking sicher?

Sichere TAN-Verfahren?

- SMS-TAN gilt mittlerweile als unsicher und nicht mehr empfehlenswert.
- Noch ältere TAN-Verfahren sollten auf keinen Fall genutzt werden.
- Online-Transaktionen einer Bank ohne TAN-Verfahren sind mit Vorsicht zu genießen, müssen aber nicht zwingend unsicher sein.

Ist Onlinebanking sicher?

Webseite oder Software?

- Mittlerweile beides sehr sicher möglich.
- Bei Webseite ist Betrugsrisiko durch Phishing und kompromittierte Endgeräte (Malware, Trojaner …) größer.
- Daher gilt allgemein, eine von der Bank empfohlene Bankingsoftware ist grundsätzlich die sicherste Methode für Online-Banking.

Ist Onlinebanking sicher?

Webseite oder Software?

- Bei Verwendung der Webseite:
  - Aktuellen und sicheren Browser verwenden
  - Nur auf Geräten mit aktuellen Betriebssystem Softwarestand
  - URL der Bank-Seite immer selbst tippen und nicht per Link aus E-Mail darauf zugreifen. Alternativ per Favorit.
  - Vor Login immer die URL im Browser prüfen.

Ist Onlinebanking sicher?

Webseite oder Software?

- Bei Verwendung der Smartphone APP:
  - Nur auf Geräten mit möglichst aktuellen Betriebssystem Softwarestand
  - Gerät verschlüsseln (Standardeinstellung bei aktuellen Smartphones)
  - Gerät und App mit Passwort oder biometrischen Merkmal sperren.
  - Aktuelle App-Version verwenden (automatische Updates aktivieren)
  - Nur die App aus dem offiziellen App-Store / Play-Store verwenden

Ist Onlinebanking sicher?

Typische Schadensfälle?

- Fast immer durch Unachtsamkeit der Nutzer.
- Angriffe per Phishing Mails mit gefälschter URL und Aufforderung zu Dateneingabe.
- Werden fast immer von der Bank übernommen.
- Kontostände werden nach Schadensfall innerhalb von 72 Stunden wiederhergestellt. (PSD2, gesetzlich geregelt)

Ist Onlinebanking sicher?

Fazit:

- Wer über Grundwissen zur persönlichen IT-Sicherheit verfügt und den Empfehlungen folgt, kann Onlinebanking sowohl im Browser, per App als auch per Banking-Software sehr sicher nutzen.
- Verbleibendes Risiko ist gering und wird bei Einhaltung der Verhaltensregeln von der Bank getragen, sollte es doch zum dann relativ unwahrscheinlichen Schadensfall kommen.

Have I been pwned?

Hacker sind wie Schmeißfliegen: Sie sind lästig, stöbern in Unrat rum‘ und übertragen Viren.

Erhard Blanck

Have I been pwned?

pwned… was?

„A corruption of the word "Owned." This originated in an online game called Warcraft, where a map designer misspelled "owned." When the computer beat a player, it was supposed to say, so-and-so "has been owned."

- *Instead, it said, so-and-so "has been pwned."*
- *It basically means "to own" or to be dominated by an opponent or situation, especially by some god-like or computer-like force.“*

Quelle: *urbandictionary.com*

Have I been pwned?

Wer hat meine Passwörter gestohlen?

- Passwörter und E-Mail-Adressen werden immer wieder in verschlüsselter Form von Online-Diensten gestohlen.
- Einen Überblick zu behalten, welcher Dienst nun schon mal ein Datenleck hatte oder Opfer eines Hacker-Angriffs wurde ist nahezu unmöglich.

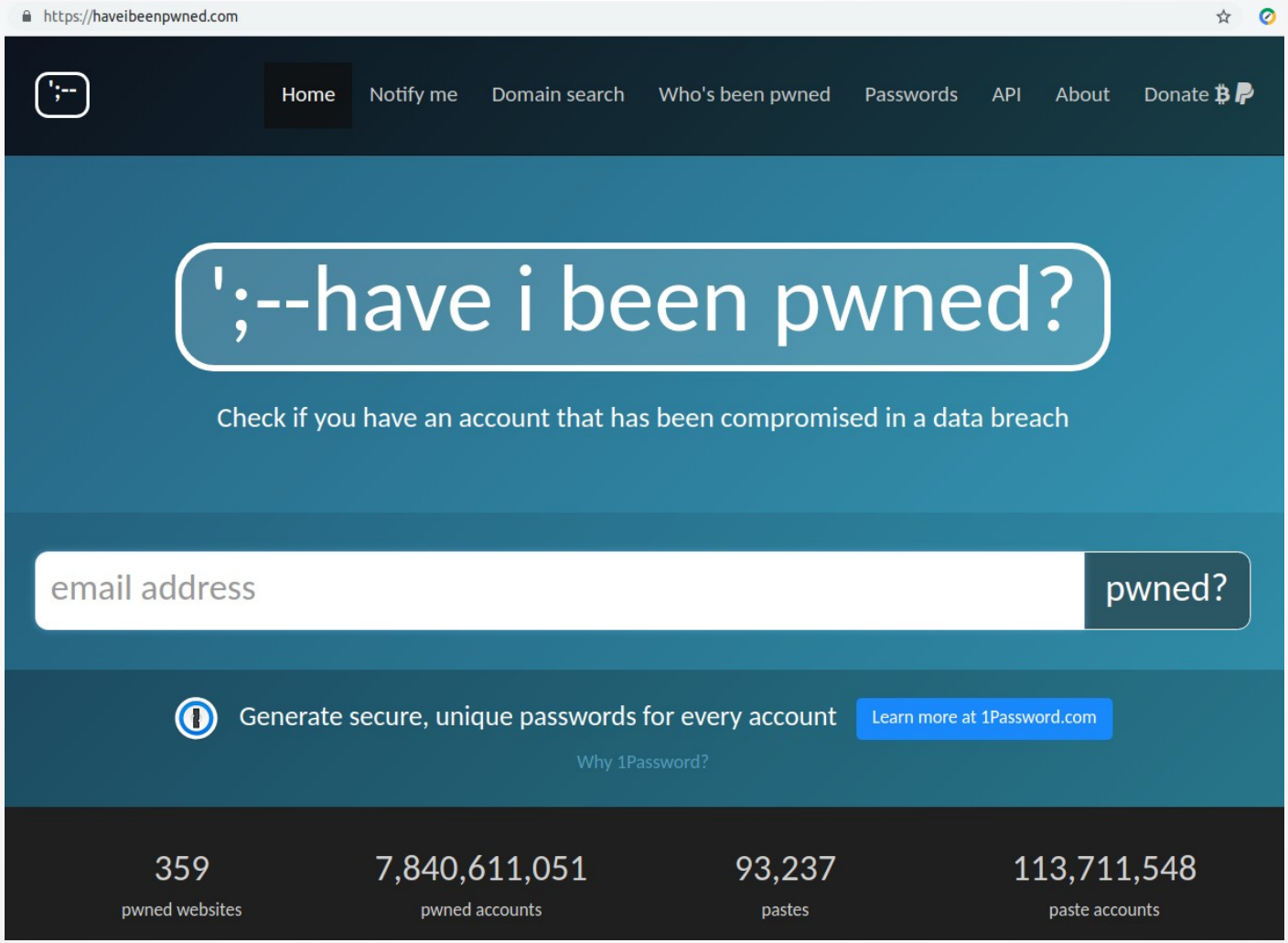
Have I been pwned?

Egal, meine Passwörter sind sicher?

- Grundsätzlich müssen „rein mathematisch“ sehr sichere (=lange) Passwörter selbst nach einem Diebstahl der Passwort-Hashes nicht geändert werden.
- Grundsätzlich sollten Passwörter immer geändert werden, und fortan nicht wieder verwendet werden, sollten sie einmal als Hash-Wert entwendet worden sein.

Have I been pwned?

https://haveibeenpwned.com/



Have I been pwned?

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

500px: In mid-2018, the online photography community 500px suffered a data breach. The incident exposed almost 15 million unique email addresses alongside names, usernames, genders, dates of birth and either an MD5 or bcrypt password hash. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords, Usernames

MyHeritage: In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, Passwords