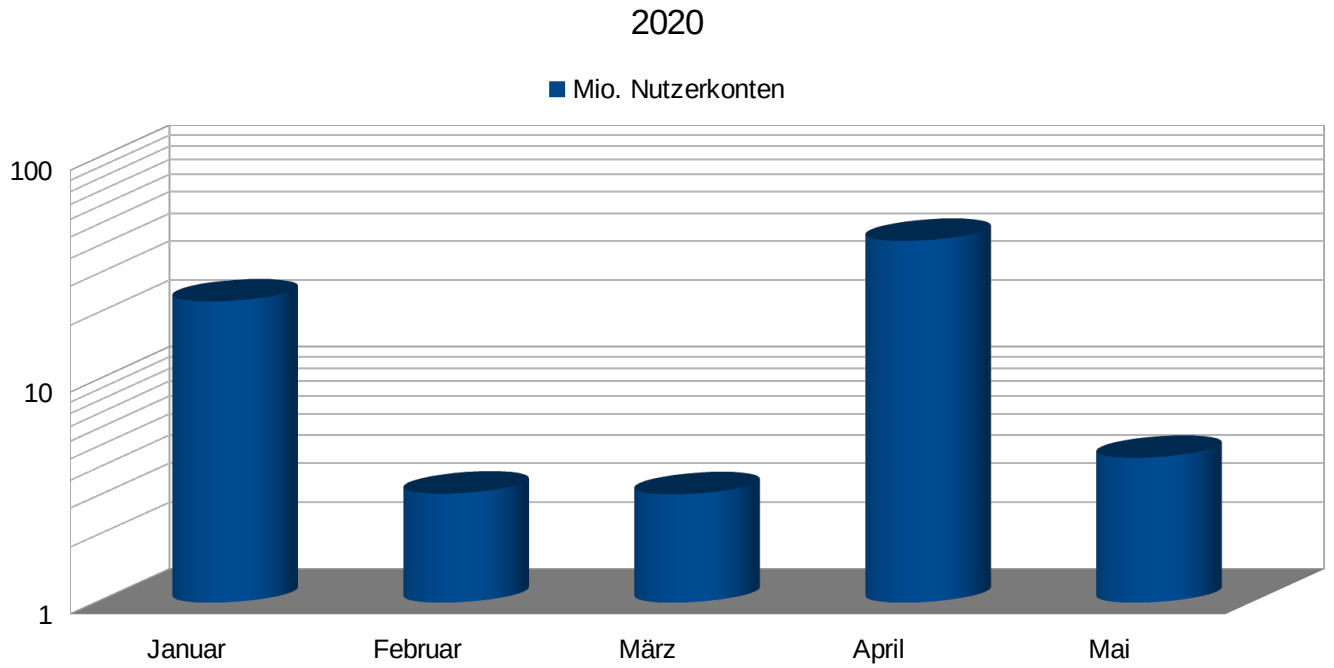
Sichere Passwörter

Agenda

- Sichere Passwörter
  - Wie werden Passwörter „geknackt“?
  - Was macht Passwörter stark?
  - Starke Passwörter selber erzeugen
- Ein zweiter Faktor macht’s noch stärker
- Passwortverwaltung

Kompromittierte Nutzerkonten



2020 bislang:

76.278.473

(Quelle: Hasso-Plattner-Institut, https://sec.hpi.de/ilc/statisics)

Passwörter-Top-10

Passwort		Häufigkeit (in ‰)
1	**123456**	8,10
2	**123456789**	3,89
3	**password**	1,89
4	**qwerty**	1,85
5	**12345**	1,38
6	**12345678**	1,17
7	**111111**	1,17
8	**qwerty123**	1,02
9	**1q2w3e**	0,97
10	**123123**	0,85
,,,	**...**	…

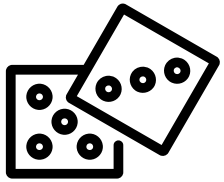
Wie werden Passwörter geknackt?

- Brute Force
  - alle möglichen Kombinationen ausprobieren
- Listen / Wörterbuch-Angriffe
  - alle Wörter aus einer Liste oder einem Wörterbuch ausprobieren
- Social Engineering
  - Phishing – Person austricksen, um Passwort zu erfahren
  - gerne auch durch Facebook, LinkedIn etc.

Was macht ein Passwort stark?

- Geheimhaltung

- Zufall

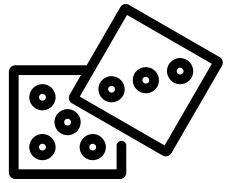


- Länge

Geheimhaltung: gar nicht so einfach …

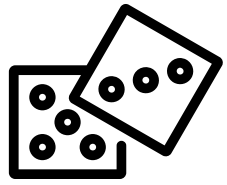
- Abhören / Abfilmen
  - Keylogger, Überwachungskameras, Handys anderer Leute, Staatstrojaner, unverschlüsselte E-Mails (Google), der Blick von hinten über die Schulter
- Schlechte Verstecke
  - Post-Its, Schreibtischunterseiten, Zettel in der Geldbörse, Cloud-Speicher (Dropbox etc.), Klartextdateien
- Social Engineering
  - liebe Menschen: Kolleg.innen, Freunde, Familie, Vorgesetzte, vorgebliche Vorgesetzte
  - nicht so liebe Menschen: Erpressung, Schmerzandrohung

Die Suche nach Entropie: Passwörter selbst ausdenken?



- Der Mensch ist nicht gut darin, sich zufällige Wörter auszudenken
- Verknüpfung von Sinneseindrücken und Vorstellung unter Einbeziehung von bereits Gelerntem → Prozess = Denken
- Problem: das menschliche Gehirn assoziiert immer
  - Beispiel auf der folgenden Folie

Passwörter assoziativ ausdenken?



- Situation
  - Ich sitze am Schreibtisch im Arbeitszimmer und esse eine Melone
  - Im Arbeitszimmer befinden sich viele Bürogegenstände; auf dem Tisch stehen z. B. ein Locher und ein Hefter sowie Stifte und der PC
- „Spontan und zufällig ausgedachtes Passwort“ durch Aneinanderreihung von Wörtern
  - **HausLocherTasteMeloneBagger**
  - Gehirn hat Gegenstände aus der konkreten Situation verknüpft
- Wörterbuchangriff möglich, da alle Wörter in einem handelsüblichen Wörterbuch stehen

Passwort vs. Passphrase

- Passwort = wenige Zeichen (oftmals ≤ 6)
- Passphrase = Aneinanderreihung von vielen Zeichen (≠ Wörter)
  - Ziel: Angreifer zu möglichst vielen Rateversuchen zwingen
  - Stärke Passphrasen = mehr Anzahl möglicher Kombinationen
- Merkmale einer guten Passphrase
  - Auf die Länge kommt es an!
  - hohe Anzahl Zeichen (z.B. 16+)
  - die Zeichen aus einem großen Alphabet auswählen (Zeichenvorrat: Ziffern, Groß-/Kleinbuchstaben)
  - zufällig ausgewählt (nicht: selbst ausgedacht)

Starkes Passwort erzeugen

- Länge + Zufall entscheidend!
- Passwort „auswürfeln“
  - Diceware
  - Würfellisten (Link am Ende des Passwortteils)
- Beispiel:
  - UAVM-3nKAEclSKDMa/WhT2En9

Zwei-Faktor-Authentifizierung

Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).

Funktionsweise Zwei-Faktor-Authentifizierung

- Teilprozesse eines Anmeldevorgangs, die zusammengesetzt werden (im Sprachgebrauch synonym)
  - Fehlen = Anmeldevorgang nicht erfolgreich
- Authentisierung
  - Benutzer.in meldet sich mittels eindeutiger Informationen an einem System an (z. B. Passwort oder Chipkarte)
- Authentifizierung
  - System überprüft Gültigkeit der Anmeldedaten und „erkennt“ Benutzer.in

Elemente
Zwei-Faktor-Authentifizierung

- Elemente
  - Besitz (z.B. Chipkarte, TAN-Generator, physischer Schlüssel)
  - geheimes Wissen (z.B. Passphrase, PIN, TAN)
  - oder Biometrie (z.B. Fingerabdruck, Retina, menschliche Gang, Stimme)
- Keine zwingende Verschiedenheit, aber in der Regel getrennte Übertragungskanäle
- In Stufen hintereinander geschaltet oder in Kombination miteinander

Arten
Zwei-Faktor-Authentifizierung: TANs

- TAN (Transaktionsnummer) / OTP-Systeme (One-Time-Passwort)
  - Einmal-Kennwort, das zeit- oder ereignisbasiert stets neu generiert wird und zusätzlich übermittelt werden kann
  - Früher: Papierlisten (iTAN)
  - Heute: TAN-Generatoren (Hardware) bzw. Authenticator Apps (Software)
  - Teilweise auch unter Einbeziehung von Transaktionsdaten (Kontonummer und Betrag); eTAN, Chip TAN
- TAN als SMS (mTAN, smsTAN)
  - Niemals dasselbe Gerät für Log-In und TAN nutzen
  - Zweite Faktor fällt weg!

Weitere Arten Zwei-Faktor-Authentifizierung

- Kryptographische Token – „Schlüssel“
- Speicherung eines privaten kryptographischen Schlüssels
  - Software-Zertifikat (bekannt von ELSTER)
  - Hardware auf einer Chipkarte (HBCI, Signaturkarten) oder einem speziellen USB-Stick/NFC-Token (FIDO/U2F).
- Biometrische Systeme: Überprüfung des Vorhandenseins von zuvor erfassten körperlichen Merkmalen (Fingerabdruck, Gesicht, Retina).
  - normalerweise nicht geheim (das Gesicht ist sichtbar)
    → Lebend-Erkennung
  - Problem: Lässt sich schwer/gar nicht ändern

How-To: Starke Passwörter merken?!

KeePass XC

https://keepassxc.org/

Vorteile

- Freie Software
- Viele Plattformen
  - Win, Linux, Mac
- Passwortgenerator
- Verschlüsselt gespeichert

Nachteile

- Masterpasswort
  - Darf nicht vergessen oder geknackt werden!
- Gefahr bei Verlust
  - „Setzt alles auf eine Karte“: PW-Datenbank gut sichern!
- Komfort
  - Kein Sync zwischen verschiedenen Geräten

Starkes Masterpasswort finden

- Passwörter würfeln mithilfe einer Passwortliste
- Warum? → Entropie!
- Vorteil: nur dieses Passwort muss man sich merken
  - Masterpasswort
- Tipp: mind. 6 Wörter würfeln

How-To: Masterpasswort würfeln

- Zubehör
  - Wortliste, aus der zufällig ausgewählt wird
    (Link am Ende des Passwortteils)
  - 6-seitiger Würfel
- Funktionsweise
  - für ein Wort wird 5-mal gewürfelt, die Zahlen werden notiert
  - dies wird mindestens 6-mal durchgeführt
    (also $6 \cdot 5 = 30$ Würfe → $6^{30} \approx 2{,}2 \cdot 10^{23} \approx 2^{78}$ Möglichkeiten)
  - Alle Wörter hintereinander geschrieben (ohne Leerzeichen)
    ergeben die Passphrase
  - Das Masterpasswort für die Passwortdatenbank nicht aufschreiben;
    durch wiederholte Eingabe ist Merken im Kopf hoffentlich möglich

Weiterführende Literatur

- Kurzweilige Zusammenfassung des eben gesagten von Alexander Lehmann: „Passwörter einfach erklärt": https://vimeo.com/138839266
- Mike Kuketz, Sicheres Passwort wählen: Der Zufall entscheidet; abrufbar unter: https://www.kuketz-blog.de/sicheres-passwort-waehlen-der-zufall-entscheidet/
- Diceware-Liste zum „Würfeln“ von Passwörtern: http://world.std.com/~reinhold/diceware.html
- Zwei-Faktor-Authentifizierung: https://de.wikipedia.org/wiki/Zwei-Faktor-Authentifizierung

– Ende Passwörter –